UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	CASE NO. CR19-00159-RSL
	)	
v.	)	Seattle, Washington
	)	
PAIGE A. THOMPSON,	)	Jane 13, 2022
	)	10:35 a.m.
Defendant.	)	
	)	JURY TRIAL, Vol. 5 of 9

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 98101

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy L. Bauer, CRR, RPR
Marci Chatelain, CRR, RPR, RMP, CCR
Official Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
nancy_bauer@wawd.uscourts.gov

INDEX

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
731	69	
741	109	
901-904	102	
905 TO 910	132	
914 THROUGH 922	132	
923	133	
924 THROUGH 927	133	
929	132	
929	133	
930	132	
930	133	

DEFENSE EXHIBITS

EXHIBITS	ADMITTED	WITHDRAWN
1100	34	

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Okay. Welcome back. Thank you, all, for being so great about your attendance.

We're continuing the direct examination of Agent Ho by Ms. Manca.

Counsel?

MS. MANCA: Thank you, Your Honor.

If we could pull up Exhibit 452, page 2, please?

WAYMON HO,
having been previously sworn, testified as follows:

DIRECT EXAMINATION continued

BY MS. MANCA:

Q. Is this an IRC chat that you reviewed during your investigation?

A. Yes.

Q. What is the date of this chat log?

A. It appears to be 2019-04-19, so April 19, 2019.

Q. And in this chat, Ms. Thompson is referring to a scanner, and in the last field it says, "39 by 36M requests."

What did you interpret that to mean?

A. So I interpreted it to mean 36 million IP addresses to scan, and "39" could refer to the number of ports to scan.

MS. MANCA: Can we pull up Exhibit 433? Can you highlight the first portion?

Q. (By Ms. Manca) And is this a Twitter message that you reviewed during your investigation?

A. Yes.

Q. What does it mean to hack into their EC2 instances, assume role their IAM instance profiles, and take over their account?

A. This is kind of, essentially, explaining the methodology that I've testified to before.

It means just that. Hacking into the EC2 instances or servers of victim companies; assuming that IAM Role, that I mentioned previously; taking over the account, and, you know, essentially, at the very end, "mirror the S3 buckets," which is the AWS sync command we've seen before.

Q. And when it says "mirror their S3 buckets," what does that mean?

A. That means to copy.

Q. And there is another sentence that says, "convert any snapshots I want to volumes and mirror the volumes I want via storage gateway." Do you know what that means?

A. I think I would need further context to know, but, essentially, it's kind of similar; copying some volume of data.

Q. Did you locate volumes of information or information you referred to as volumes on Ms. Thompson's computer?

A. Yeah. I've identified, like, S3 buckets, in the contents

of the S3 buckets within Ms. Thompson's computer.

MS. MANCA: Can we do Exhibit 416?

Can you highlight the upper third of that "Paige Adele" comment?

Let's go to 417, please.

Can you highlight the middle third, from 7/9/2019 down to 2074923452?

Q. (By Ms. Manca) Have you reviewed this Slack communication in the course of your investigation?

A. I have, yes.

Q. The Slack message says, again, looking at the very last message, "The other thing I know is that someone in one of the regions managed to figure out how to look at the IP addresses for pool traffic, I think because 20 nodes got taken out of same instant." What is she referring to with the reference to "20 nodes"?

A. She's referring to, like, 20 servers or EC2 instances.

Q. And then moving back up to the top of that message, it says, "Like the miner pool servers are regional, so it makes sense to use the ones closest to your TZ. I just never bothered for the dpkg servers, though, but I started thinking about it, and I'm wondering if, perhaps, hitting those cross-regions is tipping somebody off."

Can you explain what that means?

A. Yeah. So in this message, Ms. Thompson is explaining that

it would make sense to use servers that are closest to the mining pool servers. "TZ" standing for "time zone."

So, for example, in the previous script that we've reviewed, if a server is, for example, in the U.S. east, it would make sense to have a mine pool server also situated in the U.S. east, or connect to those.

The second statement, where she mentioned she never bothered for the dpkg servers and wondering if hitting the cross-region is tipping somebody off, we've, actually -- I've seen that in the scripts that were used for the cryptocurrency mining, specifically in the beginning of the minersetup script.

There's installations package that are being installed, and in those links, they're are all in the U.S. east region. So regardless of where these are being deployed, somehow the -- you know, the software packages are still being installed in the U.S. east region. So that's what she's referring to.

Q. And what is that cross-region functionality doing to the customers' ability to notice her activity?

A. So if the activity is going across into an area where it's not, you know, typically seen in the course of business; for example, if a server is located in Europe, and, you know, someone is seeing a lot of traffic going to U.S. east, for example, that's like an anomaly that, you know, somebody can investigate.

Q. Are you familiar with the concept of a SOCKS proxy,

S-O-C-K-S?

A. Yes.

Q. Is anything you observed in -- or you've testified about regarding Ms. Thompson's hacking process relating to a SOCKS proxy?

A. No.

Q. What's the difference between a SOCKS proxy and the vulnerability that Ms. Thompson exploited?

A. Yeah. So, you know, both of these vulnerabilities involved the use of the word "proxy"; however, SOCK proxies are fundamentally utilized differently in technology. It operates at a different level of connectivity than, you know, a reverse proxy in this example or in this case.

So to kind of give you a visualization: There's a model called the open systems intercommunication model, where it outlines several layers of how devices connect to each other.

At the bottom, you have things like the physical layer, the actual wires being plugged in, and it just goes high, higher, up to the very top, where it's an application level. "Application level" meaning, you know, the software that's installed on a server.

So with a reverse proxy, in this case, or, you know, as outlined in servers that also have WAFs, that operates at the application level.

A SOCKS proxy actually operates a little bit under that,

in, kind of, the socket level or the session level. This is, you know, a session between two computers that's being established with a SOCKS proxy; whereas, an application proxy relies on the application itself and proxying through that application.

So I know it's a very complicated thing, but the two operate on different levels of communication for devices.

Q. Can I show you Exhibit 956, without publishing it? Do you recognize Exhibit 956?

A. I do.

Q. What does Exhibit 956 summarize?

A. It's a list of IAM Roles that were identified on Ms. Thompson's computer, as well as IP addresses, and the companies and Amazon account numbers that correspond to them that the FBI has identified through legal process to Amazon.

MS. MANCA: Your Honor, we offer Exhibit 956.

MR. KLEIN: Your Honor, we object to this. We're fine with it as a demonstrative, but not as an exhibit.

THE COURT: Okay. I'll allow it to be displayed to the jury now, and we'll deal with the other issue of whether it goes back to the jury outside their presence. Okay?

MS. MANCA: Thank you.

THE COURT: You can display it out.

MS. MANCA: Let's go ahead and publish it.

Q. (By Ms. Manca) Mr. Ho, during your testimony on Friday,

there was a reference to a role called EC2_read-only. Does this document, in your other records you reviewed, refresh your memory about which company owned that IAM Role?

A. Yes.

Q. And which company was it?

A. Apperian.

Q. I'm going to return to Exhibit 645.

And there is, at the bottom, a reference to that role being EC2_read only. Whose role is that?

A. That would be Apperian or Digital.ai.

Q. And which step in the attack path is this information coming from?

A. This would be around the second step, which is obtaining the IAM Role name in order to authenticate.

MS. MANCA: Can we go to Exhibit 677?

Q. (By Ms. Manca) And so if we highlight the bottom, "Apperian EC2_read-only," this is another use of that EC2_read only IAM Role?

A. Yes.

Q. And what is the process being used with this role at this stage?

A. This is the authentication step, or it's using the credentials from the EC2 read-only role, and authenticating it using the aws_session.ssh script.

Q. I'm going to return now to the aws_commands file, which is

Exhibit 608, and I'm going to show you Exhibit 811.

Do you recognize Exhibit 811 as an excerpt from the AWS commands file?

A. I do.

Q. And do you recognize an IAM Role being used in this section of commands?

A. At the very top, there's a "42-default-instance-role."

Q. Which company's IAM Role is that?

A. 42Lines.

Q. What appears to be happening in this script?

A. So the next two commands that occur after that authentication are indicative of creating or running instances -- EC2 instances onto their environment, as well as transferring that minersetup_eth script.

Q. And what information would you need to know to determine whether that script had been successfully deployed or not?

A. Typically, we follow a large number of steps, you know, some being sending legal process to Amazon; Amazon to determine who is the owner of that IP address to confirm the company; and then, secondly, to interview the company in order to determine if they were victims of cryptocurrency mining.

Q. Were those steps taken with respect to the company 42Lines?

A. Yes.

Q. And based on that information, were you able to determine whether cryptocurrency miners were actually deployed on 42Lines?

A. Yes. It was determined that there weren't any deployed onto 42Lines.

Q. I'm going to show you now Exhibit 806.

Is this another except from aws commands?

A. Yes.

Q. Can we highlight just the top third, maybe, of this?

Do you recognize the IAM Role that's being used in this particular case?

A. Yes.

Q. Whose role is that?

A. Enghouse.

Q. And do they also go by "Survox"?

A. Yes.

Q. And so what's happening on line 5515?

A. This is the authentication step of the process where the credentials for that CICD-instance is being used to authenticate.

Q. And then what are the next commands being run?

A. So the series of commands that run after are all the run instance commands, which are to create EC2 instances. They are various degrees of the P series of Amazon EC2 Instances, which are high-computing instances.

Q. So those P3s are the type of instances being created?

A. Yes.

Q. And in what region are these instances being created?

A. It appears to be EU-west-1.

MS. MANCA: Can we go to Exhibit 808?

Q. (By Ms. Manca) So based on your review of the records in this case, whose IP address is associated with 18.208.62.195?

A. This appears to belong to a company called PowerSquare India.

Q. And which step of the hacking process are we at here for mega_metadata.txt.

A. Yeah. This is one of the first steps in which -- you know, this information shows that an IP address or server is vulnerable, so...

Q. And what about this information shows it's vulnerable?

A. That information, that "ami-id," which I've talked about earlier, shows that the correct response in talking to the Instance Metadata Service externally was successful. This is one of the indicators that established that an external device can talk to the Instance Metadata Service that's supposed to be internal.

MS. MANCA: And then can we go to page 2 of this exhibit?

Q. (By Ms. Manca) What step is this?

A. This a follow-on step in which, you know, as mentioned before, this is obtaining the IAM Role name. That's one of the required steps in order to grab the secure credentials for that role.

Q. And this is the same company?
A. Yes.
MS. MANCA: And then page 3, can we highlight the first half of that?
Q. (By Ms. Manca) What's happening on page 3?
A. So the first line is after the role name was taken. It's used in the first line in order to authenticate onto that AWS environment.
The subsequent lines including creating a key pair, which is the public and private key for SSH connections, or the remote shell connections.
The following other two lines are, again, the run instance commands, which are to create new servers, along with passing over that miner setup script.
And then the last two are changes to the security group, in which the port 22, which is commonly used for Secure Shell or remote connections, is opened onto the AWS environment.
MS. MANCA: Can we go to Exhibit 810, page 1?
Q. (By Ms. Manca) So the highlighted IEP address 13.113.12.113, which company is that associated with?
A. That belongs to the company A T Works.
Q. And what step of the hacking process is this?
A. This is one of the earlier steps in which, you know, identifying, again, that vulnerability, that ability to talk to the Instance Metadata Service.

Q. And then if we go to page 2 of this, we see that same IP address, 13.113.12.113. What step of the hacking process is this?

A. This is the authentication step where they are using that IAM Role in order to authenticate.

MS. MANCA: Go to 609, please?

Q. (By Ms. Manca) What is Exhibit 609?

A. This is a file called -- I believe it's aws_scan.txt.

Q. What information is compiled in this file?

A. This is the IAM Role name, as you can see on the right-hand side, as it relates to the IP address and phone number on the left-hand side.

Q. And there is a number, so it says "ARN: AWS: IAM," and then a multi-digit number in the middle. What is that multidigit number?

A. That is the Amazon AWS account number.

Q. Where was this file located?

A. In the aws_hacking_shit folder.

MS. MANCA: Can we pull up Exhibit 610?

Q. (By Ms. Manca) What is Exhibit 610?

A. This is another file that was found in that same directory. I believe this one is titled, "IAM_full log.txt."

Q. What information is compiled in this file?

A. It's, essentially, the same information as the last file; however, as the name suggests, "full log," it includes the full

response that the Instance Metadata Service returned to that device. It includes that same information, as well as, you know, some additional metadata information.

Q. Where was this file located?

A. In the same directory as the aws_hacking_shit folder.

Q. We've talked a lot about Exhibit 608, which is the AWS commands file.

And if we can pull that up for a second.

Approximately, how many lines of commands are contained in this file?

A. I'm not entirely sure, but it would be in the hundreds, potentially, thousands.

Q. And in reviewing these commands, what were you able to discern about Ms. Thompson's use of these commands over time?

A. Yeah. So it provides kind of a timeline of history of commands that were run on a system. But over time, you know, starting from the beginning of the commands, towards the end of the file, you can see changes or variances in the commands. Particularly, you know, them kind of evolving to be more efficient. There's less errors or less typos, and they evolve over time.

MS. MANCA: Can we pull up Exhibit 460?

Q. (By Ms. Manca) What date is this chat log from?

A. So it appears to be from July 19th, 2019.

Q. And this is a chat log from Ms. Thompson's computer?

A. Yes.
Q. Going to the first page on line 10, Mr. Ho, there is a URL link referring to nanopool.org, with some numbers and letters. What is that URL link?
A. It's linked to one of the mining accounts on Nanopool.
Q. Have we seen that specific link before?
A. The account number, yes.
MS. MANCA: Can we pull up Exhibit 855? Agent, can you expand the fields, and then go to line 57?
Q. (By Ms. Manca) And this is the spreadsheet of transactions that Vincent Kenney testified about?
A. Yes.
Q. And is the transaction highlighted in line 57 the same transaction referenced in that chat message?
A. Yes.
Q. And is there, in that transaction, an incoming to the wallet identified in that miner script?
A. Yeah. It's under column K.
MS. MANCA: Can we go back to Exhibit 460, and, Agent, can you highlight lines 20 to 33?
Q. (By Ms. Manca) So Mr. Ho, I want to highlight for you line 29, referring to "S3 bucket scrapes." What is an S3 bucket scrape?
A. So a "scrape" refers to taking down information or downloading or copying information. So line 29 tells me that S3

buckets were downloaded.

MS. MANCA: Agent, can we pull out and highlight 36 to 46?

Q. (By Ms. Manca) The first line, line 36, says, "It's impractical to have granular enough permissions as a single solution to the problem."

What do you interpret that to mean?

A. This kind of goes back to, you know, role permissions or user permissions as it relates to IAM on AWS environments.

I think what's being referred to here is to -- it's impractical to have, you know, sets of permissions be completely different for each of these different roles or user names, and saying that that is -- that's not, you know, the only solution to the problem.

Q. And there's a reference to "the number one thing that is F-ing people over." Based on your review of the evidence, what is that number one thing?

MR. KLEIN: Your Honor, I object. This calls for speculation. The document speaks for itself.

THE COURT: Well, maybe you can lay a foundation for why he would know.

MS. MANCA: Okay.

Q. (By Ms. Manca) Have you, in the forensic analysis that you've done, determined what the primary vulnerability was for the companies that were -- whose data was exfiltrated?

A. Yes.
Q. What was that primary vulnerability?
A. So this would be, as I mentioned before, that server-side request forgery attack, or, you know, the methodology of exploiting an externally-facing resource, such as a web application firewall, and using that resource to obtain internal resources that it's connected to.
MS. MANCA: Can we go to Exhibit 461, please?
Q. (By Ms. Manca) Is this another chat log that you identified on Ms. Thompson's computer?
A. Yes.
Q. What date is it from?
A. July 16, 2019.
MS. MANCA: Can we go to the second page of that document? And highlight lines 1 through 13. And can we highlight lines 14 through 21, and then can we highlight lines 22 through 28?
MR. KLEIN: Your Honor, I'm just going to object. We're just highlighting parts, and there is no testimony.
THE COURT: We're allowing the jury to read them, so I'm going to overrule the objection.
MS. MANCA: Okay. We can pull out of that. Thank you.
Q. (By Ms. Manca) Mr. Ho, what is Ms. Thompson explaining in this chat?

A. So the summary of this chat kind of has several parts, but one of them being, Ms. Thompson is providing information on how to re-create some of her activity, and providing it to this user, Nance.

In there, you see information about how to authenticate into, you know, an AWS environment once you have their security credentials. She is also providing what appears to be a link to one of her scripts, the aws_session.sh script, which we've seen before.

And further down, on line 15, she provides information on how to scrape somebody's S3 buckets, or how to copy them. That command on line 15 is similar to one that was used against Capital One.

And then at the very end, she also says that it's, you know, something that, you know, he can use, if -- but then it's not hers. That's on line 24.

MS. MANCA: No further questions. Thank you.

THE COURT: Mr. Klein, questions for Agent Ho?

MR. KLEIN: Yes, Your Honor. I just have to bring some stuff up.

THE COURT: Yeah, sure.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good morning.

A. Good morning.

Q. So I'm going to start out, picture here, and then work through a bunch of topic areas.

You spent quite a bit of time talking with the prosecutor, talking about the scanning program and the downloading of data, correct?

A. Yes.

Q. And another portion of your testimony was directed at things concerning cryptomining.

A. Yes.

Q. So first, I'm going to start out with the scanning and downloading data portion.

Ms. Thompson couldn't see any of the data that was downloaded before it was downloaded, could she?

A. That's correct.

Q. And she didn't have to decrypt any of it, did she?

A. Once she authenticated it, she did not have to.

Q. And for all of the alleged victims, including Capital One, with respect to the data that was downloaded, none of the AWS servers said she was unauthorized or forbidden?

A. No, because she authorized as one of the accounts.

Q. And isn't it true that the companies configured their web application firewalls so that anyone could use credentials?

A. I can't speak to how they would have configured or what they chose to configure for their web application firewalls.

Q. But you looked at the web application firewalls?

A. I did not.
Q. So if I asked you about how they configured their IMS roles, could you talk about that? Did you review that?
A. That was not provided to me, no.
Q. Who provided you things?
A. So we had information that was provided to us, you know, either through Amazon or through a victim. But we were never given a copy of a server that -- you know, like the web application firewall.
Q. Okay.
So after this incident happened, the FBI, or you, contacted these alleged victims about their configurations, right?
A. The FBI did, yes.
Q. And that was to notify them to change them?
A. It was to notify them that they may have been impacted by a breach.
Q. But also to get them to change them, right?
A. I was not involved in those conversations, so I don't know.
Q. You testified about some exhibits that the prosecutor showed you, where there were responses to requests that said "forbidden" or "unauthorized," but isn't it true that none of those requests succeeded?
A. Can you elaborate on what you mean by "succeeded"?
Q. Sure. You make a request, and it says "forbidden" or "unauthorized," but you actually get what you're requesting.

The request did not succeed.
A. The request did succeed because they got a response back.
Q. But they didn't get the information. They got a response that said "forbidden" or "unauthorized"; that was it, correct?
A. Yes, that's part of information that they got back.
Q. Now, talking about the scanning program and the downloading, isn't it true that someone else could have created this same program, done the same scanning, and done the same downloading of data?
A. Yes, I suppose that's possible.
Q. And isn't it also true that, in doing the scanning and the downloading, Ms. Thompson didn't have to enter any passwords to get the data?
A. She had to enter in credentials.
Q. Not passwords, though? Aside from credentials, passwords?
A. It depends on what you mean by "password."
Q. So you have a Gmail account?
A. Yes.
Q. When you log in, do you have to enter a password?
A. You have to enter in credentials, yes.
Q. Well, a password, some combination of numbers or letters you've created?
A. Sure, yes.
Q. Okay. She didn't have to enter in a password like you would with Gmail, correct?

A. As the name password, no, but secret-access token, yes.
Q. I'm not talking about secret-access token. I'm --
THE COURT: Yeah, he's answering the question.
MR. KLEIN: Okay.
Q. (By Mr. Klein) Now, in terms of what you've talked about, with Ms. Thompson scanning and downloading data, that didn't prevent any of these companies from accessing their own S3 buckets, did it?
A. Not to my knowledge, no.
Q. And it didn't prevent them using their own EC2 Instances, did it?
A. Not to my knowledge, no.
Q. And let's talk again, focus on the scanning.
There's no evidence that Ms. Thompson ever transferred any of the data that was downloaded.
A. There was evidence that she transferred it between her devices.
Q. But to any third party.
A. Not to my knowledge, no.
Q. No evidence that she ever shared it with one of these companies' competitors?
A. Not to my knowledge.
Q. Or that she used it in any way to launch her own competing business?
A. Not to my knowledge, no.

Q. No evidence she sold it?
A. Not to my knowledge.
Q. Blackmailed anybody with it?
A. Not to my knowledge.
Q. Or made any profits from it?
A. Are you specifically talking about the data, or the activity?
Q. The data, not the cryptomoney.
A. Not to my knowledge, no.
Q. Approximately how long was the data on her computer?
A. For some of them, they were on the computer since on or around March 2019.
Q. And what day was she arrested?
A. In July.
Q. And were you there at the arrest?
A. I was, yes.
Q. It was July 28th?
A. I believe so.
Q. And when you got to the arrest -- I want to make sure I got this right -- so her computer was on, the big computer we saw in that photo was on, right?
A. Yes.
Q. And then was it you who created a forensic copy at that point?
A. No. I took a forensic copy of the live memory, but not the

entire device.
Q. But at that point, you took a forensic copy of the live memory, the RAM, right?
A. Yes.
Q. And when did you turn the computer off?
A. At the end of the search -- prior to the end of the search, when we had to bag it as evidence.
Q. All right.
Now I'm going to step back and talk a little bit about your background.
What attracted you to computer science?
A. I grew up with an interest in computers, hardware and software, so that led me to pursue a degree in computer science.
Q. Okay. And did you ever build your own computer?
A. I have, yes.
Q. And you have friends who built their own computers?
A. Yes.
Q. So it's not unusual for people who are interested in computers to build their own computing rigs.
A. No, it's not.
Q. And some of your skills -- and the prosecutor did a nice job of explaining all your credentials -- some of your skills, you had classroom work, right?
A. Yes.
Q. But some of them are self-taught; isn't that right? You

would go on a computer and explore and teach things to yourself?
A. Yes.
Q. And when you go on your computer and you're looking around and doing this self-teaching, you take notes for yourself?
A. I do, yes.
Q. On your computer sometimes?
A. Yes.
Q. And do you sometimes keep track of your commands you use?
A. Yes.
Q. Both, you automate that process and you manually do it?
A. Yes.
Q. And in your own experience, when you're browsing the web, sometimes you click on a link, and it will say "forbidden" or "unauthorized," won't it?
A. Yes.
Q. Let's talk about scripts for a moment. You know what I mean by "script"?
A. Yes, I do.
Q. Not a movie script.
So people in the computer industry, or people in general, write scripts all the time?
A. Yes.
Q. And people use curl all the time?
A. Yes, that's right.
Q. And the same with SSH?

A. Yes.
Q. And are you aware that both are installed by default on Apple computers, laptops?
A. Yes.
Q. And people use proxy servers all the time, too?
A. That's correct.
Q. And people use Linux all the time?
A. That's correct.
Q. So all the tools you've testified that Ms. Thompson used are tools or programs that people use regularly: Linux, Curl, SSH, recording commands?
A. Yes.
Q. Now I want to talk for a moment about the demonstrative exhibits or the explanatory exhibits. Remember, at the beginning of your testimony, which was a while ago because we had a weekend, Friday afternoon, you gave an explanation of certain common terms or certain things that you believe happened in this case, how things worked. Do you remember that?
A. Yes.
Q. Did you create all those exhibits?
A. I assisted with creating them, but I did not create them personally, no.
Q. But you believe they're accurate?
A. Yes.
Q. Stepping back for a moment, what did you rely on to form

some of your opinions here? Like, was it things seized from Ms. Thompson? Can you give us sort of -- it doesn't have to be a perfect list, but just an overview.

A. Yes. So I reviewed the things that were identified on Ms. Thompson's devices, both the user data, data that was generated by Ms. Thompson, system data as it was generated by the operating system and other applications. I also relied on information provided by victim companies, information provided by Amazon, and other information that we've received through our investigation.

Q. Okay. Let's step back for a second and talk about proxies.

How did you learn about forward and reverse proxies?

Well, actually, can you explain what a proxy is again so we're all on the same page?

A. Yes.

So a proxy, at its very core, is kind of having an intermediary device perform some action for you. So when you're doing a request through a proxy, it will go through an intermediary, which will then go to your intended recipient, back through that intermediary, and back to you.

Q. And what is a forward proxy?

A. So a forward proxy typically involves an environment where there are computers that are within an internal network or a private network, and the data that gets sent out of that network may sometimes go through a forward proxy, in which the forward

proxy will filter that request and send it to an external recipient.

Q. I then I recall that you explained the difference between a forward and reverse proxy as whether it's going external or internal; is that right?

A. I think it happens both ways, but with a reverse proxy, the internal environment is typically on the right side. There can be cases where both are utilized as well.

Q. Are you aware that Capital One's was set up as a forward proxy?

A. I'm not aware of that.

Q. Okay.

Let's talk about TOR and VPNs for a moment.

TOR is legal, correct?

A. Yes.

Q. And are you aware that the TOR project is actually located here in Seattle?

A. I'm not aware of that.

Q. Were you aware that the Navy developed TOR?

A. Yes.

Q. And that the State Department provides funding to the TOR project?

A. Yes.

Q. And companies use TOR?

A. Yes, that's true.

Q. Universities run TOR servers?
A. Yes, that's correct.
Q. And VPNs are legal?
A. Yes.
Q. Used by companies all the time?
A. Yes.
Q. Institutions, the government?
A. Yes.
Q. And in this case, isn't it true that neither TOR nor VPN, or both combined, were needed for this scanning we've been talking about to be successful?
A. Yes, that's correct.
Q. And they weren't needed for the downloading of the data to be successful?
A. That's correct.
Q. And they weren't needed for any of the cryptomining, either?
A. No.
Q. Can we talk about Exhibit 305? And I'm going to ask that to be pulled up. This is an admitted exhibit. It's a picture of Ms. Thompson's computer.
Do you remember talking about this?
A. I do.
Q. And you spent time forensically looking at this computer, or you've reviewed it?

A. I have, yes.
Q. Now, this computer can do lots of things, correct?
A. Yes.
Q. Is it is a normal computer, but bigger. You can surf the Internet, you can play video games on it. There's lot of different purposes this computer has?
A. Yes.
Q. It just happens to be -- I think you called it a really big computer -- but a really powerful computer, maybe?
A. Yes.
Q. I'm just going through your testimony. Give me a second here.
Let's turn to Exhibit 643, page 2, please. This was another exhibit you testified about.
So do you see the word "forbidden" at the bottom?
A. Yes.
Q. So if an AWS customer doesn't want someone to see or access its files, the customer can configure its setup so it sends a message like "forbidden," right?
A. Generally, yes.
Q. Or "unauthorized"?
A. Sorry. Can you --
Q. Or "unauthorized," too, send a message like "unauthorized"?
A. Yes.
Q. Let's turn to Exhibit 670, page 0002. This was another

exhibit you testified about.

You -- in talking about this exhibit, do you remember talking about you thought -- and correct me if I'm wrong -- but Ms. Thompson was doing reconnaissance? "Reconnaissance" was your word?

A. Yes.

Q. Isn't that really just another way of saying seeing what permissions are available, with this exhibit?

A. I would say it's more akin to copying or scraping information that -- you know, that is around its environment, that you have access to.

Q. But isn't what's happening here is checking what permissions are authorized?

A. Um...

Q. Take your time.

A. So I'm sorry. Do you mean, like, permissions that are authorized for that specific IAM Role account, or just in general?

Q. This -- this -- what's happening here on this. And you're going to see my technical grasp pretty quickly, but, yes, for this specific IAM Role account.

A. So, you know, I can't -- so what I see here are commands that are run to obtain information. Now, whether or not it also outlines if something is permissible, that could be another, you know, alternative reason to do it.

But if you were to go for just permissions, you could get information about that through the IAM Role policies as opposed to trying to check which servers are available or which buckets are available.

Q. But you can do it this way, too.

A. I suppose, yes.

Q. Okay. Let's talk about the -- you've been sitting in this courtroom and listening to some of the testimony during this trial, correct?

A. Yes.

Q. So you've seen the handwritten note before?

A. I have, yes.

MR. KLEIN: Can we pull up Exhibit 1100, please? I'll use the color copy.

Your Honor, I realize we hadn't offered this into evidence, yet we had shown it before.

THE COURT: Okay. 1100 is admitted.

(Defense Exhibit 1100 admitted.)

Q. (By Mr. Klein) When did you first learn about the handwritten note?

A. A couple of months ago.

Q. Only a couple of months ago?

A. Yes.

Q. I'm going to talk now about a series of chats you were shown by the prosecutor.

Do you remember seeing a series of IRC chats, tweets, and Slack messaging?

A. Yes.

Q. And you know what IRC is?

A. Yes.

Q. And Twitter, you know what that is.

A. Yes.

Q. And Slack?

So isn't it true that all of Ms. Thompson's tweets were public?

A. The tweets were public. The direct messages were not.

Q. But the tweets were public?

A. To my knowledge, yes.

Q. And that means anybody could've -- even if you're not a Twitter user -- seen them?

A. It depends on Ms. Thompson's permissions to allow the public to view it or not, I guess.

Q. Okay. And for the IRC chats, those were public, too?

A. I'm unaware of whether they're public or private.

Q. Okay. But IRC chats can be public, and if so, they're viewable by the public?

A. If you join the channel, yes.

Q. And Slack, the same thing; if you're on the Slack, if you're in there, even if it's a message with just one person, other Slack users that are in that same group can see the same

messages, right?

A. If you join the Slack channel as a member, yes.

Q. All right. I want to talk for a minute here -- switch gears here and talk for a minute about server-side request forgery. That's "SSRF," which my tongue twists over every single time, so hopefully the court reporter will correct my mistake when I say it.

You called this an SSRF attack, right?

A. Yes.

Q. Do you know who Steve Schmidt of AWS is?

A. I know of the name, yes.

Q. He's the chief information security officer?

A. I believe so.

Q. Are you aware that he's written a letter to Congress saying this attack had nothing to do with SSRF?

A. I'm aware of one letter he sent in August 2019, where he did say he believed it was an SSRF attack. And I think there was another one in November of 2019, where he made the distinction between it being what he calls an open reverse proxy attack versus an SSRF attack. Is that what you're referring to?

MR. KLEIN: Yes, it is. Let me get a defense exhibit.

Your Honor, may I approach?

THE COURT: Sure.

MR. KLEIN: This is marked as 1102.

Do I need stickers on all the copies? I have it on the

top, and I realized this just now.

THE COURT: No.

MR. KLEIN: I'll pull this up on the screen. I'm now publishing.

Q. (By Mr. Klein) Mr. Ho, I direct your attention to the bottom of the third paragraph in the letter from Mr. Schmidt to Senator Wyden and Senator Warren.

A. Okay.

Q. Does this refresh your memory about a letter?

A. Yes.

Q. And does Mr. Schmidt say --

MS. MANCA: Objection, Your Honor. This is improper impeachment. He's testifying --

THE COURT: Yeah, I mean, if you want to call Mr. Schmidt, call Mr. Schmidt, but don't read the letter to him.

MR. KLEIN: Your Honor, he said he had looked at it, so I wanted to ask him if he disagrees with that statement by Mr. Schmidt.

THE COURT: Go ahead and ask it that way rather than read the letter.

MR. KLEIN: Yes, Your Honor.

Q. (By Mr. Klein) Do you disagree with Mr. Schmidt's statement that the attack had nothing to do with SSRF?

A. I do.

MR. KLEIN: One second.

THE COURT: Sure.

Q. (By Mr. Klein) All right. Now I'm going to direct your attention to Exhibit 205, which the prosecutor did not ask you about but has admitted into evidence.

Will you take a moment to look at Exhibit 205?

Do you remember testimony from other witnesses about this exhibit, Mr. Ho?

A. I do.

Q. Let me know when you've had a chance to look at that.

A. I've looked at it.

Q. Okay. And you've probably heard me ask this of other witnesses, but I'll ask you the same question.

If Ms. Thompson had set her web browser to use Capital One's web application firewall, or one of the other companies' using the same web application firewall setup as a proxy, couldn't she have just typed in that long HTTP address at the top, and gotten into her browser and gotten the same credentials?

A. Are you talking about the line that says, "eval"?

Q. The line that says "http:\\169.254.169.250\latest." We can highlight that. It's at the top.

Does that help you see it better?

A. Yes.

Q. It is a very long HTTP address, but you see the address I'm talking about?

A. I do.
Q. And isn't it true that if she had set her web browser to use Capital One's web application firewall, or any of the other companies' web application firewall we've been talking about or you talked about with the prosecutor, as a proxy, she could have just typed this address into her browser and gotten the same credentials?
A. She would have to do significant proxy configurations. So it's not something that's just typing in the browser. You would have to config your browser to proxy all of your traffic through that IP address, that 35.162.65.136 address. But it is potentially possible, yes.
Q. Thank you.
Let's talk for a moment about AWS --
MR. KLEIN: You can pull that down.
Q. (By Mr. Klein) AWS servers are zero permission by default, aren't they?
A. Yes.
Q. And AWS customer IP addresses are all publicly available, right?
A. Can you say that again?
Q. The AWS customer IP addresses are publicly available.
A. So the AWS IP addresses are publicly available, but who they belong to is not. So the customers --
Q. I'm not asking you who they belong to. I'm saying the

address is publicly available.
A. The external one, yes.
Q. Yes.
What is a port?
A. So a port, you know, it can be best described as kind of like an opening for a network connection at an IP address.
So there is varying ports, about 65,000 of them, that allow you to utilize network connections, programming services. You know, I've talked before about port 22, for example, being for SSH.
Q. And port 80 is HTTP?
A. Typically, yes.
Q. And port 443 is HTTPS?
A. Typically, yes.
Q. And these are common ports that people use all the time, right?
A. Yes.
Q. Thank you.
As part of the investigative work you did here, you use various forensic tools, right?
A. Yes.
Q. To look at the computers?
A. Yes.
Q. To search for information?
A. Uh-huh.

Q. And one of those tools you used is Shodan?
A. Shodan.io?
Q. Yes.
A. Yes.
Q. What is Shodan?
A. Shodan.io is a website that sometimes characterizes a web crawler. So what Shodan will do is scan external IP addresses on the Internet and identify information about them that is publicly accessible, such as port information, as well as what services may be running at that IP address.
Q. So it's a network scanner?
A. Essentially, yes.
Q. Okay.
I want to talk now -- I'm going to turn back to the Capital One data.
As part of your investigation, did you find Capital One data on Ms. Thompson's devices?
A. I did.
Q. Do you remember the volume of that data?
A. Like, the total size? Not off the top of my head, but there were millions of files.
Q. Millions of files?
A. Yes.
Q. And for someone to review that data, are you aware that -- for someone to review that data, they would need real

familiarity or subject-matter expertise about what that data was, right?

A. It depends on what the user is searching for.

Q. But it was, like, a big mess.

A. I haven't looked at it to determine if it is a mess or not, but --

Q. Maybe that's not the most technical legal term or computer science term, but it was a lot of data that was jumbled around. It wasn't easily decipherable.

A. Yes, but it can be searchable, as evidenced when Ms. Thompson searched for "Seattle" within that data.

MR. KLEIN: One second.

THE COURT: Okay.

Q. (By Mr. Klein) You found no evidence of any cryptomining on the Capital One servers, right?

A. For Capital One, no.

Q. And you spent quite a bit of time looking for cryptomining evidence, correct?

A. That's correct.

Q. You reviewed her computer, her devices?

A. Yes.

Q. You reviewed the programs and files on them?

A. Yes.

Q. You never found any private keys for a wallet?

A. Are you talking about private keys for cryptocurrency?

Q. Yes.
A. I have.
Q. Did you ever seize any cryptocurrency?
A. We did not seize cryptocurrency, but the private keys were there.
Q. But no cryptocurrency has been seized?
A. Not to my knowledge, no.
Q. Okay.
And would running the cryptomining software that you talked about with the prosecutor, would that -- that would not interfere -- sorry. Let me step back and say it a different way.
MR. KLEIN: Got to find the question, Your Honor. I'm sorry.
THE COURT: It's okay.
Q. (By Mr. Klein) As part of your investigation, you ordered Amazon Web Services abuse reports, right?
A. Not me personally, but, yes, through our investigation, we did.
Q. And they showed no mining, correct?
A. I can't speak to that because I didn't review them; other FBI members did.
Q. Are you aware from other FBI members that there was no mining shown?
A. I mean, not to my knowledge. I don't know.

Q. Do you remember sending an email on February 24th of this year in which you stated, "I couldn't find specific references to cryptocurrency mining," and discussing the abuse reports?
A. I'm not -- I mean, I would to look at it to recollect my memory.
MR. KLEIN: Your Honor, may I approach?
THE COURT: Sure.
But you did say there was no evidence of cryptomining of Capital One, right?
THE WITNESS: Yes, I did.
MR. KLEIN: And this is for other companies, Your Honor.
THE COURT: I see.
MR. KLEIN: Not just Capital One.
THE COURT: You may approach.
MR. KLEIN: I'm going to have it brought up, U.S. 15527.
THE COURT: And this is just being displayed to the witness, right?
MR. KLEIN: Yes, it's unpublished, Your Honor.
Q. (By Mr. Klein) Do you see at the top this email from you?
A. Yes.
Q. To prosecutors and agents?
A. Yes.
Q. Does that refresh your memory that you were aware of abuse

reports?

A. Yes. I think -- so what I was looking at here -- I'm trying to remember my context -- I only reviewed for, you know, the term for "cryptocurrency" or "mining." But the rest of the abuse reports were reviewed by somebody else. I looked for, as I mentioned, specific references.

Q. Would it help to refresh your memory if it was unredacted that redacted portion?

A. Sure.

MR. KLEIN: Your Honor, we'd ask for an unredacted copy of this.

THE COURT: Well, I don't want to deal with it right now. Move on to another topic.

MR. KLEIN: Okay.

Q. (By Mr. Klein) I'm going to direct your attention to -- there was a chart you were shown -- that is Exhibit 850 -- by the prosecutor. Can we please pull that up?

Can you explain, again, what your understanding of this term is?

A. So this chart is just the timeline of the Ethereum account balance over the months.

Q. And that's for a specific public address?

A. Yes. That's that 0x5a86 wallet.

Q. And other people could have sent mining awards to that same address, correct?

A. It's possible, yes, if they put it in their application.
Q. And so other people could have gone to Nanopool -- you testified earlier that Ms. Thompson was sharing a script for mining on IRC, correct?
A. Yes.
Q. Other people could have gone in and used that same script or used the same wallet address, right?
A. I'm unaware of a script where it included the exact 0x5a86 address.
Q. You can see the mining award going to that address, but you can't tell who is specifically earning the mining award, right?
A. Not to my knowledge, no.
MR. KLEIN: That's it, Your Honor.
THE COURT: Okay. I'll come back to that other issue later.
Ms. Manca, do you have any redirect for Agent Ho?
MS. MANCA: I do. Thank you.

REDIRECT EXAMINATION

BY MS. MANCA:
Q. Mr. Ho, is it fair to characterize cryptocurrency mining as separate and apart from scanning activity?
A. Yes.
Q. How is the cryptocurrency mining related to scanning activity, if at all?
A. Are you talking about for this case specifically?

Q. For this case, thank you, yes.
A. So both of the methodologies for both scanning and for cryptocurrency mining are related because, in order to get to the cryptocurrency mining part, that sort of scanning activity has to occur, and then the multiple steps after the fact, you know, authenticating and deploying the miners, that's what makes the cryptocurrency miners relate to this case.
Q. So the path between stealing data and cryptocurrency mining, where does that path diverge?
A. That path diverges kind of at the very end. So once Ms. Thompson had access after scanning, after getting the role name, after authenticating, and figuring out the permissions, that is where it diverges, whether there's data taken or cryptocurrency miners are deployed, or both, in some cases.
Q. What determines whether there's going to be cryptocurrency mining, data theft, or both?
A. I would say it would be dependent on the permissions of that specific IAM Role.
Q. What is a "credential"?
A. So a credential is used to authorize in a system. Typically, when you think of a credential, you think of it as a combination of a user name and a password. In other cases, it may be a key and a secret access key. It may also pertain to, for example, the public key and private key authentication used for SSH.

Q. So are passwords the only type of credential or authentication in the world of technology?
A. No. There are multiple ways to authenticate, and credentials can mean a large number of things.
Q. Is it common in technology to use something other than a password as a means of authentication?
A. Yes.
Q. Can IRC chats be private?
A. They can be, if you are talking directly to an individual instead of on a channel.
Q. Is there any disagreement between -- you were asked questions about Steve Schmidt of Amazon and a letter he wrote describing this attack. Do you recall that?
A. I do, yes.
Q. Is there any disagreement between you and Steve Schmidt about the technical aspects of this breach?
MR. KLEIN: Objection; foundation, Your Honor.
THE COURT: Yeah. You can say why would he -- did they discuss it, are you talking about that? Or are you just talking about you see what he did, and --
Q. (By Ms. Manca) Have you read -- you were provided a letter by the defense. Have you read that letter before?
A. Yes.
Q. Does the letter contain a description of the technical aspects of the breach?

A. I do.
Q. Do you agree with the technical aspects described in that letter?
A. I do.
Q. What do you and Mr. Schmidt disagree about?
A. I disagree about the naming convention that's used and the statement that it is not a server-side request forgery attack.
I think, fundamentally, whether Amazon chooses to name it an SSRF or open reverse proxy attack, the underlying methodology that's explained both in my testimony and by Amazon is the same.
In fact, there is also an Amazon incident response report that was provided to one of Ms. Thompson's victims, where they also concluded that the attack factor was an SSRF attack.
Q. You testified --
MS. MANCA: If we could show Exhibit 205, and highlight the first quarter of that. Thank you.
Q. (By Ms. Manca) You were asked a question about whether it would be possible to enter this kind of command into a web browser; do you remember that?
A. I think I was asked whether or not, if he used a proxy and then connect to that 169 IP, that was the specific question, but, yes.
Q. So what changes would have to be made to an ordinary web browser in order to execute this command?
A. You would have to config your proxy settings to proxy

through that 35 IP address. But it would also depend on how that external IP address is configured to allow that to occur on a web browser as opposed to on a curl command.

So, I mean, I don't have, like, a direct answer for that.

Q. You were asked questions about Shodan?

A. Yes.

Q. And you described it as a network scanner or Internet scanner?

A. Yes.

Q. Okay. When Shodan is scanning, what information does it provide to the people being scanned about its scanning activity?

A. So when Shodan scans an IP address, typically, in the request that it makes to those IP addresses, it leaves some information that identifies that it is Shodan.io. This is seen in other network scanners that may be used by universities or others, where it identifies itself as either Shodan or something else.

Q. How does a scanner identify itself as a university or a Shodan program?

A. So, I mean, there's a lot of ways, but usually it's in the request that's included. You know, either they'll make changes to the User-Agent string, where they say that it's coming from Shodan's devices, or they'll leave some sort of note that identifies that it's Shodan.

Q. Do you know why Shodan and universities clearly identify

themselves as that program at universities?
A. I can't speak for all of them, but, generally, it's to identify themselves to the scanned IP address that they are being scanned by one of these scanners.
Q. Does Shodan harvest security credentials?
A. Not to my knowledge, no.
Q. Does Shodan download data?
A. They download the responses that they send, but actual data that's, like, user data, as opposed publically available data, no.
Q. And does Shodan install scanner on the computers it scans?
A. Not to my knowledge, no.
Q. You were asked some question about evidence of cryptocurrency mining, and there was a reference to specific report or an Amazon abuse report?
A. Yes.
Q. What specific words were you looking for in that report?
A. Generally, just "cryptocurrency" or "miner."
Q. Did you find those words in that report?
A. Not to my knowledge, no.
Q. Have you found other evidence of cryptomining in other information provided by Amazon?
A. Yes. So instead of looking at the abuse reports, I looked at the billing records for the victim companies that we've identified, and then we correlate that with creation of EC2

instances that align with commands run by Ms. Thompson on her computer, and various other things.

MS. MANCA: Thank you.

THE COURT: Any questions in these areas?

MR. KLEIN: Yes, Your Honor, one second. Just a few.

THE COURT: Sure.

MR. KLEIN: Can you pull up Defense Exhibit 1014? But don't publish. Your Honor, it's not admitted.

Your Honor, this is a previously shown exhibit.

THE COURT: Okay.

RECROSS-EXAMINATION

BY MR. KLEIN:

Q. You talked about Shodan for a moment. Are you aware that certain people at Capital One thought that Ms. Thompson was doing a confession scan?

MS. MANCA: Objection; lack of personal knowledge.

THE COURT: Well, remember, a lawyer's questions are not evidence, so -- but I will allow the question. You can answer, if you know.

A. I don't know.

Q. (By Mr. Klein) Did you ever check to see if any of the scans you thought were run would qualify as confession scans?

A. I did not review those.

THE COURT: So, again, the lawyers' questions are not evidence, so there's nothing to take away from that, other than

he doesn't know.

Q. (By Mr. Klein) You talked for a moment about, in response to the prosecutor, your view of the divergent path of what happened here, sort of your view of the evidence, how Ms. Thompson's -- how you viewed things happened.

And with regard to the cryptomining, was that done on a preexisting EC2 instance, or a new EC2 instance?

A. To my knowledge, it's typically done on a new EC2 created by Ms. Thompson.

MR. KLEIN: Nothing further.

THE COURT: Okay. I'm going to send you to lunch now, and please ask you to be back by 1:10. You're on the same floor now. Isn't that nice? Cuts down on the travel time.

We'll get started about 1:15, but I'm going to deal with this one last issue. So you are excused. Thank you.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Thank you. Please be seated.

So I'm not sure, Mr. Klein, if you still want to push that issue with the email, or are you, like, "Maybe I'll leave that alone"?

MR. KLEIN: Your Honor, let me have a moment to talk to Mr. Hamoudi about it.

THE COURT: Sure.

I'll tell you what. We'll take the break, and you guys

talk about it over the lunch hour, and then if we need to start back up with Mr. Ho for this, we will do it, and if not, we won't.

MR. KLEIN: In the meantime, maybe it would make sense for Your Honor to see an unredacted copy. We haven't seen one yet.

THE COURT: You've never seen an unredacted copy?

MR. KLEIN: No. That was the focus of our motion to compel an unredacted copy.

THE COURT: Do you have those available here?

MS. MANCA: Not with me in court, but in my office, I do.

THE COURT: Sure. So bring one up at 1:10 or so, and I'll look at it. They'll tell me if they want to push it. I won't show it to them unless they push it, and we'll see what goes from there.

All right. So we have a couple of witnesses this afternoon, one remote?

MS. MANCA: Two remote, Your Honor. We're going to put both of the remote witnesses, Clint Popetz and Eric Brandwine back to back, immediately after lunch.

THE COURT: Okay. Victoria, is that going to work?

THE CLERK: Yes.

THE COURT: Okay. We'll be back to start at 1:15.

(Court in recess 11:58 a.m. to 1:16 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE CLERK: Please rise. Court is again in session.

THE COURT: Please be seated.

Can we get rid of that? It's like an older version of myself.

You did that on purpose, Tony, didn't you?

Okay. You still want to push this thing about the email?

MR. KLEIN: Your Honor, we do to an extent. And I'll explain.

THE COURT: Okay.

MR. KLEIN: We have obviously filed our motion to compel, which you denied. When I asked the witness, he clearly would have been helped, in my opinion, by looking at the rest of that email. That's why we had originally raised the issue with the Court.

THE COURT: Sure. But what was the actual question you were asking him?

MR. KLEIN: I was asking him about the bottom part of that email.

I have every exhibit, except that one.

Anyways, I was -- I'll find it. I was asking him about the bottom part of that email.

Oh, here it is.

And -- which is Bates stamped USA 15527. And at the bottom

it says, I couldn't find specific references to cryptocurrency mining, though.

THE COURT: Right. That's the point you wanted to make, that he didn't find evidence of cryptomining.

MR. KLEIN: And then he pushed back.

THE COURT: And then he said, I'd need to see the whole email to understand.

Now, you're not really suggesting that there was no evidence of cryptomining, are you?

MR. KLEIN: I'm not suggesting that through that question, Your Honor, but what I'm trying to get to is that when he ordered the AWS abuse reports, they did not show any evidence of cryptocurrency mining.

And then he reinforces one of our points, Your Honor. And then he wanted to -- he said he indicated he would have been helped by the redacted portion.

THE COURT: Okay. Here's the unredacted to refresh yourself, okay? And then when we bring the jury back, you can ask him.

MR. KLEIN: Your Honor, can I look at, though? I might not want to ask him once I look at that.

THE COURT: Sure. You can look at it.

MR. KLEIN: Thank you.

THE COURT: I mean, look, too much is being redacted over here. And then, frankly, what we did on Friday afternoon

ex parte didn't need to be ex parte. So let's get on the program more with each other about -- you know, this -- what you were talking about Friday afternoon with the AWS is something they should have a role in, too. And as we go forward, they're going to, so...

MR. KLEIN: Your Honor, one point about that "too much being redacted," they redacted a lot of stuff for the other witness, John Strand, who they intend to call tomorrow. And my concern is we may run into the same issue with those redactions because I do plan to cross him on potentially some of those same emails.

THE COURT: Okay. I'll be ready.

That help?

AGENT HO: Yes.

THE COURT: Okay.

AGENT HO: Yes, Your Honor.

THE COURT: All right. Let's go get the jury.

MR. KLEIN: Well, may I approach, Your Honor?

THE COURT: Yeah, sure.

MR. HAMOUDI: Your Honor, to your point about yesterday's matter, I have no objection to that transcript being made available to the government --

THE COURT: Okay.

MR. HAMOUDI: -- provided they...

THE COURT: You know, actually, since Mr. -- Agent Ho

is going to be here, why don't we do the other stuff, then we'll come back to that.

MR. KLEIN: Okay.

THE COURT: Okay?

So you can go into the audience and...

Thank you.

THE CLERK: Do you want me to admit the witness before I get the jury?

THE COURT: "Admit" meaning bring 'em -- yeah, let's change that picture for sure.

(Off the record.)

THE COURT: So while we're waiting for the jury to come in, then, Amazon's response had sort of the standard contract.

MR. HAMOUDI: Yes, Your Honor.

Do you want me to address it?

THE COURT: Well, why wouldn't that be good enough?

MR. HAMOUDI: Well, I just want a copy of it, and I'd be able to establish that that is the standard contract that involves all the companies, and I'm good, Your Honor --

THE COURT: Okay. So once, you know, Andrew and Jessica and Tania get to see what we're talking about, maybe they'll agree to a stipulation to that effect.

MR. HAMOUDI: Okay. Great. Thank you.

THE COURT: Yeah.

Are our 'zoner lawyers still here?

UNIDENTIFIED SPEAKER: Yes, Your Honor.

THE COURT: Okay. We'll get to it.

Here comes the jury.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Does the government want to call its next witness?

MS. CULBERTSON: Your Honor, the government calls Clint Popetz.

THE COURT: Mr. Popetz, would you stand up and raise your right hand?

You've got to stand.

THE WITNESS: Okay. You won't be able to see me, though.

THE COURT: That's all right, we'll hear you.

THE WITNESS: Okay.

THE COURT: Go ahead and listen to the oath.

THE CLERK: Raise your right hand.

CLINT POPETZ,
having been first duly sworn, testified via Zoom as follows:

THE COURT: All right. Thank you. You may be seated.

You know, one of the advantages to Zoom, I did a Zoom trial, you know, is you really can get witnesses from everywhere.

The defense has stipulated and agreed that this witness can testify remotely, because Ms. Thompson has an absolute constitutional right to have the witnesses here in the courtroom, but they have cooperated in this manner.

Where is Mr. Popetz?

THE WITNESS: I'm in Toronto, Ontario, in Canada.

THE COURT: Yeah. But my buddy Bill Downing just did a case where one witness was in Paris, another one was in Croatia, and it's -- it works pretty well, so...

All right. So, Ms. Culbertson, you want to -- or do we have -- Victoria needs to ask you to spell your last name, so please go ahead, Victoria.

THE CLERK: Thank you, Your Honor.

If you could please state your first and last names and spell your last name for the record.

THE WITNESS: Sure. It's Clint, and the last name is Popetz, P as in Paul, O, P as in Paul, E as in Edward, T as in Thomas, Z as in Zebra.

THE COURT: Thank you.

Go ahead, Ms. Culbertson.

DIRECT EXAMINATION

BY MS. CULBERTSON:

Q. Good afternoon. Can you hearing me okay?

A. Yes.

Q. Where do you currently work?

A. 42 -- I currently work for 42Lines Canada, which is a subsidiary of 42Lines U.S. that was created last fall. Previous to that, I worked for 42Lines U.S., and then co-owner and founder of 42Lines U.S.

Q. Okay. And what is your current title now at 42Lines Canada?

A. I'm general manager.

THE COURT: What does 42Lines stand for?

THE WITNESS: It doesn't stand for anything. I took the name because the original printing press had 42 lines on it. And so the constraint of technology defined how books were printed for long after.

THE COURT: I didn't know that. Thank you.

Go ahead, Ms. Culbertson.

Q. (By Ms. Culbertson) I think you may have already said this, but when was 42Lines founded?

A. 2009, April of -- no, May 1st, 2009.

Q. Okay. And you were one of the founders?

A. That's correct.

Q. Okay. What did you do as CTO of 42Lines?

A. I did everything from programming, architecture design, hiring, managing of technical staff, setting policies, creating our sort of technical direction. Basically, all of the technical side of the company was under my control.

Q. And what does 42Lines itself do? What kind of business is

it?

A. So at the time primarily -- of these events primarily it was a services company working mainly in the higher ed sector doing -- on contract programming to build different solutions for different universities, non-profits, mainly centered on online learning.

Since then, there's been a development of an -- of a -- of a piece of a software that's sold more -- less as a con- -- less as contracted engineering and more as a direct softwares and service product. But that is a separate part of our overall portfolio, so...

Q. In 2019, did you oversee a team of employees?

A. Yes.

Q. Okay. And approximately, how many people did you oversee?

A. Probably between -- directly and indirectly, probably around 20. Directly, I had three direct reports, and then beneath them a total of 20 people.

Q. In your role as CTO in 2019 and in your current role as general manager, do you have knowledge of and experience with computer coding and computer scripts?

A. Yeah.

Q. Going back to 2019, did 42Lines use Amazon Web Services in 2019?

A. Yes.

Q. When did 42Lines start working with AWS?

A. Really early. I would say probably we were migrating things from on-premises cages into AWS in -- by 2011.
Q. And what does 42Lines use AWS for?
A. We use it for a variety of things. We run our software as a service inside it. We use it for instances that serve as web application servers, for database servers, for internal software that's used for a variety of purposes, managing, ticketing, managing internal storage of documents. Basically, any time we need to provision any sort of instance, we use AWS.
Q. Can you give me a sense, just a general sense, of how many instances 42Lines was running in 2019?
A. I mean, I could find out for you very quickly, but I don't know. Probably, at that time, including the ones we ran internally and the ones we run for customers, probably 40 in various subaccounts.
Q. And are you aware of the roles and permissions that related to those instances?
A. Yeah.
Q. How did you first learn that 42Lines was involved in this case?
A. So there was an image that was snapshotted of a directory listing of files that was making its way both around Internet forums that we -- this kind of a community of people that do this kind of work, and there were Internet forums. This was -- an image was posted of -- of people who had been involved in

this hack. It was also posted to news sites.

And our -- because our name starts with the number 4, it sorts to the top of the list, and so we were in the top few lines. And so whenever someone screenshotted this document, ours was always one of the first things that showed up. And there's no other entity or company named 42Lines, so it was pretty clear that we were involved in it.

Q. Do you remember about when you first saw this screenshot that you described?

A. I honestly don't. I can't recall. Sorry.

MS. CULBERTSON: Okay. Jessica, can I ask you to pull up 408?

Q. (By Ms. Culbertson) We're going to try and share a document with you here.

A. Sure.

Q. This is Exhibit 408, which has already been admitted.

A. Yep, that's the one.

Q. Okay. That's the post that you were referencing just now?

A. Yep.

Q. And can you see at the top there, 42Lines.net?

A. Yep.

Q. So that's what you're talking about?

A. So this is what we saw posted within -- in Slack forums. There was even a Webmonsters forum, which is just a group of people who do operations.

I also saw it in an online search for the hack and -- to verif- -- see if it was showing up in news articles and it was.

Q. Did seeing this in 2019 or whenever you saw it, did it cause you concern?

A. Oh, yeah, yeah, I immediately was curious. Not a terrible amount of concern because the -- you can name a file anything, right, so someone could do a dig on us, which is a public service about what domain information is and save the result. So we didn't know what was in that file, but we knew it couldn't be very much because it was not very large. But we knew that if there was -- had been a hack and if it was verified that some people had lost private information and our name was on that list that it was a concern.

Q. So what did you do next after you became aware of this post?

A. Well, we did some digging about -- about the -- the sort of nature of the hack because at this point it had already been -- it had already become public, what it was. And we were quickly led to -- pretty much the whole community knew immediately what was going on and that it was an AWS metadata hack. And AWS responded to it and we responded to it. But also we sort of tried to reverse engineer based on the size of that file what it could be.

And we also reviewed all the security policies and made sure that no one was -- we looked at access logs to find out who

was accessing service when and if we had seen any kind of -- we have a lot of monitoring that's in place on all of our servers, so we were relatively certain that there wasn't a full intrusion.

So, for example, we would know if someone had --

Q. Sorry. I'm sorry to cut you off.

A. Yeah. Okay. I could -- I -- yeah. Sorry.

Q. I will ask you more about that, but I also just want to --

A. Yeah. That's okay.

Q. -- at some point did you meet with law enforcement?

A. The FBI contacted my vice president of operations, and my vice president of operations contacted me about it, and then eventually I talked to that same agent.

Q. Okay. And when you talked to that agent -- do you remember the name of the agent you spoke with?

A. Yeah, Joel Springer, I think. I'm really bad with names, but -- is that correct?

Q. Well, Joel is correct.

Might it have been Special Agent Joel Martini?

A. Yeah, it's a Joel -- it's a Joel of some sort. Sorry.

Q. And did you agree to some follow-up actions after speaking with the FBI?

A. Yeah. We agreed to -- well, there was several meetings, and I wasn't in the first couple, but my -- when I talked to him, I agreed to both send him the digging that we had done, and

then in exchange, he sent us the digging that you guys had done, so that -- mainly, we wanted to know what was in that file. Even though it was very tiny, it was -- for example, it could have been a compressed security key or something that would have given further access, but --

Q. Okay.

A. But actually we -- okay, I'll stop. I answered that.

Q. That's okay.

And when you say you did further digging into what they had, so is it fair to say you wanted to look at a copy of the file the FBI had?

A. Yeah. I wanted to look at that. We also looked -- there was a possibility -- he suggested the possibility to me that cryptohacking or cryptomining instances had been launched on our account, and so we wanted to go verify if that had happened. And we -- so we went looking through audit logs from the past two years just to see if there had been any difference in the types of instances that had been launched.

Q. Okay. And we'll talk about that more in a moment.

I'm first going to show you documents -- it's Exhibit 730. It's also already been admitted. Pull that up for you.

Do you recognize that document?

A. Yeah. That's the contents of the -- so the top-level thing that you showed previously was what we call a tarball, which is an archive. And inside that archive, those are two files each

with those names.
Q. And is this --
A. This is a directory listing of that -- of that archive.
Q. And is this a directory listing that Special Agent Martini sent to you?
A. Yes.
Q. Okay. So, Mr. Popetz, I know you have a document in front of you on your end that is labeled Exhibit 731.
A. Yeah.
Q. This has not yet been admitted, but if you could take a look at that document and let me know if you recognize it?
A. Sure.
Yep.
Q. Is this also a document --
A. Yeah. So --
Q. Is this also a document that Special Agent Martini provided to you?
A. Yes. So this is the con- --
Q. Hang on just --
A. -- what I'm looking at is the contents of one of those files.
THE COURT: Okay.
MS. CULBERTSON: Sorry. The government moves to admit Exhibit 731.
MR. HAMOUDI: I don't have an objection, Your Honor.

THE COURT: 731 is admitted. It can be displayed.

(Government Exhibit 731 admitted.)

Q. (By Ms. Culbertson) We're going to pull that document up so we can see what you're talking about.

Okay?

A. Do you want me to describe this?

Q. Yeah. Could you tell me just in general terms what this shows?

A. Right. So Amazon has a set of APIs -- I don't know how deep -- it has a set of commands you can run that are used to describe information about the resources that they've allocated upon your behalf. So when I say I launch an instance, I run a command and Amazon creates that provisions, that instance, and give me information about it. And when I want to describe that instance, I run the command that's called EC2 describe-instances, and this was the output of that command.

If you run it with only a single instance, it tells you a description of one. And if you run it without any, it gives you all of them. So what this is is a description of all of the instances in a given region in Amazon.

So that's why each of those file names was a region name, east and west, and then this is the contents of one of them showing metadata information about the instance that has been created by me.

Q. Okay. So just to clarify, make sure that I understand what

you're saying, this is output of a described instance and it's showing 42Lines instances?

A. That's correct.

Q. Was this kind of output of data designed to be publicly available?

A. No.

Q. Who was supposed to be able to access this kind of output of data?

A. So, typically, operations people use this. For example, if you were going to run a script to walk through the instances in your cloud to verify something about them or to test whether a given port was reachable on them or to just generally do maintenance and monitoring of them, you would run this. And then you would take the results of each of these pieces and feed them into another piece of code.

So you could use it just as a cursory inspection, you could feed it into a script, but, yeah, it was meant to be used by our system administrators.

Q. Okay. So by your system administrators, you mean by 42Lines' system administrators?

A. Yes. Correct, correct.

Q. How would a 42Line system administrator access this data? What would they have to do to get access to this data?

A. So they would either be on a provision instance -- they would either access a provisioned instance using, for example,

SSH, so that they were -- then we say that they're on the instance, they've logged into it.

Q. What is -- just quickly, can you briefly describe, what is SSH?

A. SSH is a secure protocol for accessing remote machines. So when you think of logging into your computer, SSH allows you to log into a remote computer.

Q. So, I'm sorry, I interrupted you, you said they would either be?

A. No, that's okay. They would either be SSH into a remote computer that had the privileges to run this, or if they were on their home laptop, there's a whole system using multifactor authorization and hardware keys for them to obtain the privileges from EC2 from Amazon in order to run this EC2 command.

Q. Was --

A. So each operations engineer has a laptop, the laptop has hardware keys that we send them, USB keys, and then we manage the permissions and the rotation of credentials such that at any given time with their password and with that hardware key there, and with their multifactor code, they're able to do certain things. And this would be one of the things they could do.

Q. In reference to an SSA connection, are you familiar with the term "key pair"?

A. Yes.

Q. And can you explain that to me, that term?

A. So, yeah, in SSH, you would -- we would play -- on the instance itself, we would have a copy of -- so it's a little bit difficult to describe how key pairs work, but, essentially, it's a secure exchange of -- cryptographic exchange so that passwords do not necessarily have to be exchanged. It's a way of verifying who you are without relying upon a password. And it's a -- so it's a -- it's a very long -- not very long, but an amount of gobbledygook text that you couldn't memorize that gets placed on the server. And then you have a corresponding piece of it on your client. And when you go to connect to the server, it says, who are you, and you say, I'm this person, and it says please present it, and you send them your part, and they have your other part. And using a mathematical operation, you can determine if the two match.

So it's the sort of underlying security mechanism that almost all -- most all two-party exchanges of information happen with in the world at this point.

Q. Okay. Thank you for that explanation, I appreciate it.

So turning back to the data here that we see on Exhibit 731, was this data important to 42Lines?

A. It isn't -- it's not an -- so it's not an asset, nor is it -- or it is a customer's data, it's not data that is private or that I would consider a trade secret. It is, however, data that -- like so when you build a -- when you build an Internet

security or any kind of security infrastructure, it has multiple layers. The first layer is just that they don't know how -- an attacker doesn't know how your entire system is provisioned, so that's the sort of obscurity layer. After they know how it's provisioned, what its IP addresses are, and what the different devices within it are doing based on names of them, then you have all kinds of different layers of security, including, you know, how can I access the machine, what ports are open on it, et cetera.

And so it's not information I want people to have because it represents that first layer. If you know what -- how were submitted and what instances are up and what instances are doing what, then you have more of an opportunity to attack them. So this isn't information we share because no one needs to see it. And so if they -- and if it were widely available, if it were, for example, public information, then it would be one less layer of security around.

But the least -- the least -- it's sort of that -- it's like, for example, if -- if someone wants to know the cert of all public machines that were running and what their IP addresses are, they actually can figure that out because most of them are reached by SSL, which means we have to have a key, we have to have a cert for them, and that cert is governed by -- bought by a separate -- from a separate company. I know they're registered and they can be looked up, so --

Q. Okay. So -- sorry, I'm just --
A. It's not super critical, but it's not something I want to share.
Q. That's fine. And I didn't mean to cut you off, I just -- once you start talking beyond my level of understanding, but --
A. Yes. That's fine. Sorry.
Q. So to make sure I understand what you're saying, having this data out in the public presents some danger to 42Lines' security; is that correct?
A. It's just a -- it's just a risk, yeah. It's just -- I mean, one, it's -- yeah, it's a risk because it's a description of internal architecture that otherwise is not available.
Q. Okay. Very good.

So earlier you talked about steps you took internally to look into what happened here, why this data was out in the world. I think you mentioned reviewing internal logs. Is there anything else that you reviewed in the course of that investigation?
A. Correct.

Yeah. I mean, we did a full audit of roles and what privileges each role were given and what users had been using, what roles.

At that time, Amazon did not have alerts concerning whether someone who was not in your account was using a key from your account, so it was a little bit harder to do. Since then, it's

become much easier to make sure this can't happen. But, yes, at the time, we reviewed an enormous amount of stuff.

Q. Were you able through that review to determine what allowed access to these S3 buckets?

A. Yeah. So we have -- we have servers that are facing the public. One of them, in particular, is -- runs a piece of software called Jira. Jira is a product that you use for ticket management for -- let's say a customer files a bug or we do an internal feature request, we file a ticket, so -- and that ticket goes through various stages. That server had a security hole -- or that piece of software had a security hole in it, it isn't software we write, but it is software we rely on, that piece of software had a security hole whereby you could cause it to hit an internal -- you could cause it to proxy a request. Proxy means you do it on my behalf. So you could contact that server and ask that server -- piece of software on that server to relay the request on your behalf to a different place on the same server.

At that time -- at the time -- this is going to get complicated fast, so stop me if you need me to explain --

Q. So let me just pause you there for a moment.

So you said a request was proxied to another place in the internal server; is that fair?

A. It was proxied to that same server, but a different port on that same server.

Q. Different port --
A. So you would hit the external server on, say, SSL port, which is 443, which is the standard way you talk to the web. And then beyond that, you -- that piece of software erroneously and as a security hole was willing to relay that request directly to another port on the same machine.
Q. In order to make that request through the proxy, would you have to be using a 42Lines role?
A. No. So that's the most exterior level of the vulnerability is that the -- that piece of software, Jira, did not need you to have any permissions in order to edit that part. That part was basically open to the world for proxying.
Q. Okay. Does having access to a 42Lines role credential, at what stage in this process does that come into play?
A. So in order to run this command in this 731, you had to have that privilege. So in order to be able to do anything with Amazon, you have to have a role. And in order to get the role, you need a key for the role. And so the whole trick here was how to get a key for a role that would let you do something with Amazon on your behalf.
Q. Okay. Do you know what role -- what role was used to run this command --
A. Right, right, I do. So there's -- so you can have roles -- there are different kinds of roles. There are roles that you have by virtue of who you tell Amazon you are. That's the case

when I use my laptop to talk to Amazon. Amazon says -- I say, Amazon, I'm this person; Amazon says, great, here are the things you can do.

When you have an instance, which is, for example, this ticketing software was running on an instance, a computer in the cloud, that instance has its own role by virtue of just being an instance. And it has a set of things it can do.

In this particular case, that instance had a very limited role because we knew that it wasn't going to do anything except just live. It was servicing web requests, but it wasn't trying to do anything complicated inside Amazon, so it had our default instance role.

And so what -- the hack here is that there's a metadata server on every instance. When you are trying to do any work on an instance, sometimes you need to know who am I. Like you might write a script that says I'm going to talk to Amazon, but first I need to know who I am and what privileges I have. And so you ask the metadata server, and the metadata server says, okay, your role is this, your IP address is this, these are the things you should know about yourself.

The problem here is that that metadata service in the original Amazon structure was not locked down. It wasn't required -- you weren't required to do anything except make a git to it, make a web request to it. Since then Amazon has changed that and you have to make a post and you have to have a

key and there's a whole set of processes, but at the time, it was very vulnerable.

Q. Okay. So --

A. And so what happened --

Q. Sorry. I know we keep talking over each other.

So I think you mentioned that this default role that this instance was running, if that's the right way to characterize it, had limited permissions; is that right?

A. That's correct.

Q. Can you tell me what those permissions were, if you know?

A. I don't have the exact enumeration of them. They were -- one of them was able to describe instances, as you can see here. Another one was being able to list instances. Another one would be able to -- they had access to read top-level S3 buckets or a set of buckets that we used to store things. So S3 is like folders in the cloud. It's where you store data, right. We have a set of S3 buckets that contain software images to run, meaning not data of a customer or internal data, but they contain the images, like you would launch an instance and then that instance might go to an S3 bucket and grab a piece of software it needs to run, download it and run it. So that role I know, at the least, has the ability to do these minimal set of things, describe itself, describe the instances, list S3 buckets, things like that.

Q. Do you know if it had permission to run new instances?

A. It did not.

So that was -- the -- another piece of evidence that you sent me was the batch history of the --

Q. We're actually going to pull that up next.

A. Okay. Okay. All right. Sorry.

Q. So we can go ahead and pull that up. That's Exhibit 608.

Okay. So this is the first page of 608. And you used the term "batch history."

A. Yeah. I mean, it could be any -- but I'm guessing it's that.

So when you run commands on a Linux-based machine, every command that you run stores what you did in a history file. And you can see on the left there's a number like 32, 33, 39, that's just the number of the -- in the line in the history file. And then to the right of that is what command was run.

So I presume this is a history file taken from the computer of the person who was doing this or from an instance that they were using outside our instances to do this. And so --

Q. Okay. I'm going to point you to specific areas --

A. Sure.

Q. -- in this document.

So if we can turn to page 6 and look at line 891. Sorry, it's small. We're going to see if we can blow it up a little bit.

891.

Okay. Do you see the command that's shown at that line?
A. Yes.
Q. Okay. And do you --
A. So this is -- yeah, so this is -- curl is a program that simulates as if you were a web browser, you're -- it's making a web request. And this is using the proxy that's on the -- that was our Jira server. So you can see proxy, and there's an IP address. And I don't have an IP address, but it's too long ago, but -- and I don't normally memorize IP addresses, but I know enough based on our digging that this was our Jira server, 443 is the port, but that's them hitting the web on our computer server. And then they're telling it to proxy -- to -- you're zoomed in a bit, but if you zoom back out a little bit.
Yeah. Thank you.
So they're using -- they're using as a proxy that Jira server open port, and they're asking it to hit the metadata server. So that http thing that has latest/meta-date/iam/security-credentials, it's trying to get its own security credentials from that metadata server.
Q. Okay. And then --
A. And that's the successful hack right there. That line is the sum total of the hack.
Q. Okay. And the 42-default-instance-role, is that the 42Lines default role we've been talking about?
A. Correct. That's correct.

Q. That had the limited permissions?

Okay. Turning to page 12 of this document at line 1867, do you recognize the command at 1867? It's near the bottom of the page.

A. Yeah. That looks to be the same thing. I don't know if it -- if that is a different IP address on the same Inserver because it could -- because I don't -- I don't fully recall, but that's the same thing. It could be a different server, for example, we run Confluence, which is another piece of software by that same company, but it's essentially trying to do the same thing, it's trying to gain -- and I can't -- I have no way of knowing which of these failed and succeeded because we don't have the output. Obviously, one of them succeeded, because they were eventually able to list -- list the instances, so at some point one of these did not fail and returned the credential.

Q. Okay. And finally, I'm going to turn to page 21 and -- the bottom of 21 and the top of 22, so we'll scroll between them a little bit. But let's start at the bottom of 21 at line 4885.

What do you see there?

A. I see 4890 -- oh, 85, sorry.

Yeah. This is the same thing. This is attempting to retrieve metadata or trying to use the metadata server via the proxy to obtain -- obtain credentials.

Q. Okay. And then in the following line 4886 we see described -- well, it looks like it may be a misspelling of

inferences, but a correction of 4887 describe-instances?
A. Yep.
Q. Do you recog- --
A. So that's -- yep. And that's the two files that you found on the tarball on the archive. So that's successfully -- they successfully obtained the credentials. I'm assuming the awssession.sh is a command that then puts -- either puts them in the environment or puts them in a file in the AWS config directory that allows you to use them.

And then -- and then AWS EC2 describe-instances with the region is the thing that we saw the output of in the other file.
Q. Turning to the next page, the top of the next page, 22, there's another command at 4894?
A. Uh-huh.
Q. Do you see that?
A. So this is them attempting to assume another role within 42Lines in order to attempt to have more privileges. So -- and there are two roles that are listed there, rundeck-instance-role and ops-pi-instance-role. Both of those are an attempt to take this -- take the role that you have and to obtain the privileges of another role. Some roles are able to switch roles to other roles and some are not.

In this particular case, this role is not. And so we don't have the output here, but it was not successful, at least based on our -- our analysis of the roles after the 7.

Q. Okay. Your analysis of the permissions that the roles had --

A. Correct.

Q. -- during your investigation?

A. Correct.

Q. Okay. Once 42Lines figured out that all of this was happening, did it fix the problem that allowed for this to happen?

A. Oh, yeah. Yeah. So one is just disabling filtering so that no one can reach the unfortunately open proxy on Jira. But the other is that we locked down via firewall what could access -- what could access the port of the metadata server, and then we switched -- once AWS made it available, we switched to the newer form of the metadata severer so you can't just hit it in order to get the information.

MS. CULBERTSON: Okay. I'm going to step away from the podium for just one moment to ask my co-counsel if there's anything else.

(Off the record.)

MS. CULBERTSON: That's all the questions I have for you, but stay online because the other side gets to ask you some questions now. Thank you.

THE WITNESS: Sure.

THE COURT: Mr. Hamoudi, who represents Paige Thompson, will cross-examine now.

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Mr. Popetz, how are you?

A. I'm good. Thank you.

Q. How's the weather over there?

A. It's gorgeous for the three months of the year that it's gorgeous.

Q. That's good to hear.

Have a question, You don't have any records in your possession that detail the actual access to your servers, do you, the CloudTrail logs?

A. We do have CloudTrail logs going back pretty far away, so we know, for example, that the server itself did not have any login access. There are certain things that we felt -- we keep track of and certain things we don't. So the only -- the logs that we have that show the access to the server were -- were Apache logs for the Apache server itself, which we do -- we keep for a certain amount of time before we delete them.

Q. So you don't have an exact date when this happened is what I'm asking you, because the CloudTrail logs would evidence an exact date when --

A. I do. I do have the -- I do have the Jira logs that show the exact date of the intrusion via Jira, the hits to Jira.

Q. Okay. And before you locked down the web access firewall, it allowed access; correct?

A. That's correct.
Q. And you, yourself, the first time you were interviewed by the FBI was early this year; correct?
A. Yeah. My VP of engineering spoke to the FBI prior to that, but the first time that I spoke directly was earlier this year.
Q. Okay. And you configure your identity access management role; correct?
A. I don't personally configure, I -- so IAM is configured via a software called Terraform. Terraform is a software where you feed in the descriptions of what you want to have existing in Amazon, and then it causes those to match your descriptions, so those change over time as we -- so, for example, this entire setup is substantially different several years later because our architecture is always evolving.
Q. But you -- your company configures those roles; correct?
A. Yes, that's correct.
Q. And your company sets permissions as to what someone can or cannot do with those roles; correct?
A. That's correct.
Q. And your company configures who can have access to S3 buckets and who can download data from those S3 buckets; correct?
A. That's correct.
Q. And once you learned about this information in the media, you corrected the problem; is that fair to say?

A. That's correct.
Q. And --
A. We didn't change the -- to be clear, we didn't change the permissions of the role because the permissions of the roles are correct, what we changed was the hole that allows both Jira to access the metadata server and for the metadata server to be able to be accessed by anyone outside the machine.
Q. Is that because you exercise or implement the principle of least privilege?
A. That's correct.
Q. And can you --
A. That principle was always implemented.
Q. And can you talk to the jury about what that principle means?
A. Right. So there are layers of security, security is an onion. I talked about one of them already, which is just the easy one, which is obscurity. The next layer is that no server should be able -- no piece of software or server or anything should be able to do something that it doesn't need to do. So you don't give access to a piece of software or to a server or to a human to do something that they would never need to do, so that even just by accident or by a hack that bad things happen.
So, for example, this particular server was configured to have a role that didn't allow it to do anything terribly interesting. It wasn't -- for example, it wasn't allowed to

launch new servers, anything that would have cost me money, but it -- but it did have the ability to do a certain set of things --

Q. Okay.

A. -- because it had to.

Q. And then one final question: Do you have any evidence that your data was shared with anybody by my client, Ms. Thompson?

A. The only data I know that was shared is the data that's been presented here, which is -- which was I don't -- I don't know what it means by sharing; I know that -- I know -- I didn't see this data until the FBI sent it to us; however, the files themselves -- the size and -- the size of the tarball that was found matches the size of this when it's compressed, so I know that it is the same data that was on that directory. I have no evidence -- I don't know what else the person did with these files. I have no way of knowing.

MR. HAMOUDI: Okay. No further questions, Your Honor. Thank you.

THE COURT: Thank you very much, Mr. Hamoudi.

Anything else?

(Off the record.)

THE COURT: Ms. Culbertson.

MS. CULBERTSON: Nothing further, Your Honor.

THE COURT: All right. Thanks very much, Mr. Popetz. We're signing off now.

THE WITNESS: Thank you.
THE COURT: Thank you.
THE WITNESS: Okay. Take care.
THE COURT: Bye.
(Off the record.)
THE COURT: So we're going to do the next witness, who is also remote.
MS. MANCA: Your Honor, the government calls Eric Brandwine.
THE COURT: Okay. You can bring Mr. Brandwine in.
THE CLERK: Mr. Brandwine, if you could please turn on your video.
He is in the Zoom, just doesn't have his video on.
MS. MANCA: Might need to take a break and check with him and get him on the video.
THE CLERK: I sent him a chat to start his video, but I can't start it with him.
MS. MANCA: Just one moment.
THE COURT: Can he hear us at all?
THE CLERK: He probably can.
Let me see if I can send a chat to him.
MS. MANCA: Here it is. Okay. Good.
THE CLERK: I think he's on.
THE COURT: Hello, can you turn your video on?
There we go.

THE WITNESS: It is on.

THE COURT: Great.

Okay. Mr. Brandwine, I'm Judge Lasnik. Could you please stand and raise your right hand, and my clerk will give you an oath to tell the truth, okay?

THE WITNESS: Okay.

THE CLERK: Please raise your right hand.

ERIC BRANDWINE,
having been first duly sworn, testified via Zoom as follows:

THE WITNESS: I do.

THE COURT: Okay. Thank you. Please be seated.

And Assistant United States Attorney Jessica Manca will have ask you some questions.

Go ahead, Ms. Manca.

MS. MANCA: Thank you.

DIRECT EXAMINATION

BY MS. MANCA:

Q. Good afternoon, Mr. Brandwine. Can you please tell us where you would?

A. Yes, I work for Amazon.

Q. What do you do for Amazon?

A. I am a vice president and distinguished engineer on the AWS security team.

Q. What is a distinguished engineer?

A. Distinguished engineers are our most senior technical

individual contributors. They are expected to have broad impact across the company.

Q. When did you join Amazon?

A. I joined Amazon in December of 2007.

Q. And what did you do before joining Amazon?

A. I was a contractor at the Mitre Corporation working for a group at the Department of Justice.

Q. How long have you been working in technology and network security?

A. Probably on the order of 25 years.

Q. Roughly, how many people at Amazon Web Services are working on security?

A. Within the AWS security org, it's several thousand.

Q. You've been doing security, as you said, for about 25 years. Do you think any security system is impenetrable?

A. No. I don't believe that any security system is impenetrable. Security is about understanding and mitigating risk, not about guarantying security.

Q. I'm going to show you Exhibit 952, which has already been admitted.

Do you recognize that exhibit?

A. I do.

Q. What is it?

A. This is a note that one of my colleagues handed to me during an internal conference. I believe it was on May 20th,

2019, but I may be off by a day or two.
Q. You said "an internal conference"; what do you mean by that?
A. So the senior technical individual contributors, the principal engineers, get together. It's typically annually, although COVID has interrupted that pattern. And we all just get together and meet new people and share best practices; typically, a two-and-a-half-day off-site.
Q. Where was this conference held?
A. This one was held at the Sheraton in downtown Seattle. I don't recall the exact address.
Q. And is this a conference where the general public can attend?
A. No. This is Amazon employees only, and only specific invited Amazon employees.
Q. And the area that you received this note, was that a restricted -- an area that was open to the general public or restricted to Amazon employees?
A. It would have been restricted to Amazon employees.
Q. Do you remember who gave you the note?
A. Unfortunately, I don't. It was an unusual event at the time, but not as important as it wound up being. So I don't recall the name of the person, but I do remember that they were one of my fellow principal engineers.
Q. What made it unusual to receive a note like this?

A. Well, this has never happened to me before or since. I've never had an experience like this. I've never had someone report a security issue or a suspected security issue with a physical submission. Usually, they come in to one of our teams and they come in electronically.

Q. When you received this note, was it immediately apparent to you what the note was saying?

A. It was not immediately apparent to me what the note was saying.

Q. Was it immediately apparent to you whether it was talking about a vulnerability of some kind?

A. So, yes, it was immediately apparent that it was talking about a vulnerability. SOCKS is a common proxy software used on the Internet, and an open SOCKS proxy is a type of misconfiguration that would be familiar to any security engineer. The fact that there was some sort of misconfiguration and likely a security exposure here was obvious.

Q. How easy would it be for a large company to find a misconfiguration if they were just told that they had a misconfiguration?

A. Given the IP address, you could start trying to track down the owner. However, in a large corporation, inventory can be a challenge. It can be difficult to know who is the owner of a given IP address or what system it's associated with.

Q. For a large company running on AWS, what is the universe of

potential misconfigurations you could have?
A. I don't know that we know yet the potential universe of misconfigurations that are possible, because the largest service that we offer, the Elastic Compute Cloud, EC2, allows customers to run general-purpose machines, typically running windows or Linux operating systems. And so every possible misconfiguration you could have in any data center on earth could occur somewhere in Amazon Web Services.
Q. Do you consider this note to be a responsible disclosure to Amazon?
A. I do not consider this to be responsible disclosure.
Q. Why not?
A. In all attempts at responsible disclosure that I've previously participated in, the reporter left a return communications channel. Many of these submissions were anonymous. It was obviously a throwaway Gmail account or something like that. And so we don't know who the reporter was, but there was always a way to reach out to them and say, how did you find this, why is this important, why is your concern about this so high. We believe we fixed this, can you verify that we've repaired it. And so there's absolutely no way to follow up on this.
Q. Why is that follow-up an important part of responsible disclosure?
A. The key to responsible disclosure is that the reporter is

trying to make things better, they're trying to improve the security stance of whatever it is that they're reporting about, and so closing the loop there, guarantying that the issue that was reported is either confirmed as no issue or confirmed as fixed is really the underlying goal of responsible disclosure.

Q. So what did you do with this note when you received it?

A. I took the picture that you are showing me here using my cell phone, and I immediately forwarded it to our on-call alias saying I was just handed this note, I do not know its source, can you please investigate.

Q. There's a thumb in this photograph, is that your thumb?

A. That would be my thumb.

Q. Were you involved in AWS's response to the Capital One breach in July of 2019?

A. I was, but only peripherally. I served as an escalation point, basically.

Q. And when that breach occurred and you heard about it, did you immediately connect it to this note?

A. I did not.

Q. And to this day, do you know whether this note is related to that breach or not?

A. Honestly, the only linkage I have between this note and the Capital One issue is the fact that this note is coming up at this trial.

MS. MANCA: No further questions. Thank you, Mr.

Brandwine.

We're going to have cross-examination by --

THE COURT: Mr. Klein, the attorney for Paige Thompson, will have some questions for you.

Mr. Klein?

(Off the record.)

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Hi, Mr. Brandwine. Can you see me?

A. Yes. I can see and hear you. Thank you.

Q. I'm Brian Klein. I'm one of Ms. Thompson's attorney. Good afternoon.

So I want to start out with a question for you, which we're going to put a version of the note on the screen.

MR. KLEIN: 1100, please.

Q. (By Mr. Klein) Are you able to see that, Mr. Brandwine?

A. I am.

Q. Okay. And that's -- I'll represent to you that's just a color copy of the same note you were discussing earlier.

So this conference was in Seattle in May of 2019?

A. Yeah.

Q. And do you see that IP address there, 35.162.65.136?

A. I do see that IP address.

Q. Okay. And there is a way to search AWS customer IP addresses, isn't there?

A. Yeah. It is very straightforward, given an accurate timestamp, to map a given IP address back to a customer account.
Q. Okay. And are you aware that this note was passed along to Capital One during this time frame?
A. I was not aware of that.
Q. Okay. But would you be surprised that AWS could take this note and then find out which customer it was and provide it to them?
A. I would not be surprised if AWS could determine which customer owns this IP address.
Q. And so you talked about when you got this note. What else do you remember about when you received this note?
A. I asked my colleague who handed it to them, and they refused to give me any more information. I asked if there was any way to follow up, they refused to give me any more information. They said I was just given this and asked to hand it to you and so that's what I'm doing. And so that's what I recall. I took the picture and I sent it to our on-call.
Q. Okay. So your colleague told you that they were asked to hand it to you by someone else?
A. Correct.
Q. And that was your colleague. So when you talked about responsible disclosure earlier, this wasn't a stranger off the street who met you in front of the Sheraton and gave you the note, was it?

A. No, it was not, but it was also not the person who had any knowledge of the issue.

Q. But it was someone whose name you could have tracked down or found or asked at that time; correct?

A. Correct.

Q. And so if you had gotten that person's name and you passed this note on, Amazon could have spoken with that person if you had gotten their name; correct?

A. That speaks to our effort to identify the reporter, but not the reporter's intent to disclose responsibly.

Q. Yeah, I'm not going to that right now.

I'm just saying, if you had gotten this person's name later, Amazon, AWS, could have -- it's one of their employees, they could be speaking to them; correct?

A. Yeah. If I had thought to remember who had handed me this note, we could have established communication with them about this issue.

MR. KLEIN: Okay. Nothing further, Your Honor.

MS. MANCA: I don't have any follow-up based on that.

THE COURT: Okay. Thanks very much, Mr. Brandwine. Where are you testifying from?

THE WITNESS: I am located in Northern Virginia.

THE COURT: Okay. Thanks so much. Appreciate you making yourself available. Bye now.

Okay. We ready with another witness?

MS. MANCA: Yes, Your Honor. The government calls John Roundy.

(Off the record.)

THE COURT: Mr. Roundy, please come into the open area of the courtroom here.

And could I ask you to raise your right hand and listen to the oath?

JOHN ROUNDY,
having been first duly sworn, testified as follows:

THE COURT: Please have a seat up here.

THE CLERK: If you could please state your first and last names, and spell your name for the record, please.

THE WITNESS: It's John Roundy, R-o-u-n-d-y.

THE COURT: Thank you, Mr. Roundy.

Go ahead, Ms. Manca.

DIRECT EXAMINATION

BY MS. MANCA:

Q. Sir, where do you work?

A. I work for Enghouse Interactive based out of Phoenix.

Q. And what does Enghouse Interactive do?

A. We actually provide contact center software for our consumers and also serve a management component.

Q. What are survey management components?

A. It's when -- like, for instance, when you finish a call, we'll say, stay on the line for a survey, and then we'll pass

you off to a survey to rate the customer experience.
Q. How long have you been with the company?
A. 22 years combined between the company we acquired and Enghouse, seven with Enghouse directly.
Q. What company was acquired by Enghouse?
A. Information Access Technology is where I came from.
Q. And are you familiar with a company called Survox?
A. Yes, ma'am.
Q. What is Survox's relationship to Enghouse?
A. Survox was acquired to give us a component for survey management in our contact center software.
Q. What year did Enghouse acquire Survox?
A. The end of 2017, beginning of 2018.
Q. What is your present job for Enghouse?
A. I'm the director of cloud operations and services.
Q. What does the director of cloud operations and services do?
A. So I oversee all cloud operations for our hosted products for our customers and our equipment for our customer service team.
Q. What did you do before -- actually, strike that.
So we were talking about surveys after contact call centers, you know, how was your experience. How does Survox play a role in that component of the business?
A. So they're a hundred percent the survey engine, so they're the ones that manipulate the data that's being received via the

phone or web and giving -- reporting back to the customers of what the results of the survey was.

Q. So that then you interact with customers by providing them information about what their customers told them about services?

A. That's correct, yes, ma'am.

Q. Okay. Approximately, how many customers do you have?

A. Enghouse total or Survox?

Q. Enghouse total.

A. Probably 1,600, 1,700 total.

Q. Mostly corporations?

A. Yes, ma'am.

Q. Does your company use Amazon Web Services for cloud computing?

A. Yes, ma'am.

Q. How long have you been using AWS?

A. Let's see. Survox moved to it probably nine years ago. As a company on the whole, we're probably eight and a half, nine years.

Q. When was the first time you realized that your computer systems had been breached?

A. When we received the AWS bill for March, which we received the first part of April.

Q. What year was that?

A. 2019.

Q. Can I show you, without publishing, Exhibit 901?

And before your testimony, I also showed you 902, 903 and 904; is that right?

A. Yes.

Q. Does your job for Enghouse include reviewing and paying invoices?

A. Reviewing them, yes, and approving them to be paid.

Q. Okay. And do you recognize Exhibits 901, 902, 903 and 904?

A. Yes, ma'am.

Q. Were these invoices received on or about the date listed on the invoice?

A. Yes, ma'am.

Q. How do you use these invoices in your business?

A. It's for controlling of costs as well as performing budgetary requirements for the future years.

Q. Do you rely on these invoices as an accurate accounting of money you owe to Amazon?

A. Yes, ma'am.

Q. Is your company's regular practice to keep such invoices?

A. Yes, ma'am.

Q. And were these invoices kept in the course of your regularly conducted business?

A. Yes, ma'am.

MS. MANCA: Your Honor, we offer Exhibits 901 through 904.

THE COURT: Mr. Klein.

MR. KLEIN: No objection, Your Honor.

THE COURT: 901 through 904 are admitted into evidence, may be displayed.

(Government Exhibits 901-904 admitted.)

MS. MANCA: Can we publish Exhibit 901? Can we highlight the top half?

Q. (By Ms. Manca) So what month is this bill for?

A. It was for -- it would be April. It's March 1st through March 31st. And the bill was due on May 3rd.

Q. And what was your reaction when you received this bill?

A. Honestly, shocked, very shocked.

Q. What was shocking about it?

A. Our typical run rates were $7,000, $8,000, and receiving a bill for $53,000 was quite scary.

Q. What's a run rate?

A. Run rate is the typical usage we use in a single month.

Q. What was scary about this invoice?

A. It went from $6,000, $7,000 to $53,000.

THE COURT: Kind of like filling up your car at the gas station.

THE WITNESS: Yeah, especially that.

Q. (By Ms. Manca) How does that affect your operating budget?

A. It puts us upside down, honestly, with the budget, because we're only budgeted for X amount per month, and having a bill that's 10, 15 times, that puts the budget upside down. I mean,

that's the amount of money we would spend almost in a year.
Q. What did you do when you received this bill?
A. First thing we did is contact Amazon to say, what happened, because we weren't for sure. And then we worked with the Amazon representatives to determine what we needed to do to correct it.
Q. What did they tell you this bill was based on?
A. It was based on systems, were spun up in Ireland, their P series instances, that were extremely expensive. And so we asked them, what do we need to do to terminate them. And then they walked us through the termination practice to get rid of them.
Q. And did Amazon eventually refund you this money for this bill?
A. Yes, ma'am.
Q. You mentioned that P3 servers had been created on your account. Did you ever use P3 servers in your business?
A. No, ma'am.
Q. What about P2?
A. No, ma'am.
Q. Okay. What kind of instances do you typically use?
A. We usually use the M3 series, or we're using T1 or T2 micro series.
Q. What's the difference between those series of instances and the P series of instances?
A. Extreme compute power is the biggest one. Also, the P

series has graphical processing units in them as well, which the other series do not.

Q. Okay. And which region -- when you are creating instances for your own business use, can you control where these instances are created?

A. Yes, ma'am.

Q. Which regions do you typically use when you create instances?

A. U.S. west and U.S. east.

Q. Have you used Dublin, Ireland or the region in Dublin, Ireland for any instances?

A. No, ma'am.

Q. When these instances were created, you mentioned that the way you solved the problem was to terminate the instance?

A. That's correct.

Q. How did you go about doing that?

A. We used the Amazon web page to get to the dashboard to terminate the EC2 instances that were created.

Q. When you go to the dashboard for Amazon, is that something you use in your business to control things on Amazon web services?

A. Correct; it's the gateway to the Amazon engine.

Q. Okay. What credentials do you need to access this gateway to your Amazon account?

A. User name and password and also MFA token.

Q. What is an MFA token?
A. Multiform authentication, which is just a code that's generated on your cell phone that is required for you to gain access to your account.
Q. So these instances that were up and running on your account, did you have access to them?
A. Physical access to them, no.
Q. What kind of access did you have?
A. We could stop them and terminate them is all the access we had.
Q. So that's why you took that course of action?
A. Yes, ma'am.
Q. Could you see what kind of programs were running on those instances?
A. No, ma'am.
Q. So after, you know, you got this bill and the money was refunded, did you later determine that you had been breached in a different way?
A. We weren't aware of a breach of -- data-wise until October, when the FBI came to our office in Phoenix.
Q. Getting back to this bill and then the data breach, did you have an understanding of how the breach occurred?
A. Yes, ma'am.
Q. How did it occur?
A. When we contacted Amazon Web Services to determine where

the instances were spun up and how it was done, we were informed that there was an IAM Role that was associated to a specific EC2 instance. That EC2 instance was compromised, so the key to access that system was compromised. And then once they had access to that machine, they could actually do a temporarily -- a temporary request to get another key or a temporary key, which allowed those instances to be spun up from the CLI tool.

Q. Do you remember which role was used in this compromise?

A. Yeah. It's used for continuous improvements, so CICD instance, and so it's continuous improved and continuous deployment.

Q. What is this role used in your typic- -- what is this role used for in your business?

A. So it's specifically used by our research and development teams. Once the code set's been built, it actually will pull it, build it, deploy the machines for them, reducing the overall workload on the development team.

Q. And so the role -- what permissions does this role have within your AWS environment?

A. It has permissions to pull API keys, spin up new instances, EC2 instances, as well as deploy software.

Q. Is this a role that is used by people or by machines?

A. It's a hundred percent by machine. It's an automated task.

Q. Did you intend for that role to be used by members of the general public?

A. No, ma'am.
Q. How did you close the vulnerability in this case?
A. The first thing we did is shut down the machine that was compromised, which was Staging Green [sic]. Once that was done, we removed the AMI role and rekeyed and provided a new user for our development team.
MS. MANCA: Can we show Exhibit 806.
And maybe magnify 529 to 533.
Q. (By Ms. Manca) So do you recognize on line 529 cicd-instance?
A. Yes, ma'am.
Q. What is that?
A. That's an IAM Role.
Q. Okay. And in lines 5516 down through 5541, but we're just highlighting to 5519, there's a command there that says "ec2 describe-instances," and then "ec2 run-instances." Do you recognize those commands?
A. Yes, ma'am. It's a CLI command to pull instance types, as well as to run 'em.
Q. What's a CLI?
A. Command line interface.
Q. So are these the same commands that you would use if you were logging into your AWS account to run instances?
A. Not directly, ma'am, no.
Q. Okay. How would you do that?

A. We typically log on to the web portal, which is the dashboard I referenced earlier, to control our EC2 instances. But for our deployment practices, we do use the CLI command because it's easier.

Q. Okay. Are these commands that you or anyone at Enghouse or Survox issued?

A. For these specific ones, no, it's using PC -- P3 series that we do not use.

Q. Did you receive a set of data from the FBI? So you mentioned that this cryptojacking, you worked with Amazon in the March-April 2019 time frame?

A. Yes, ma'am.

Q. And then you were later contacted by the FBI about data from your company in October of 2019?

A. That is correct, ma'am, yes.

Q. Did the FBI send you data related to this case?

A. Yes, ma'am, they did.

Q. And when you received that data set, were you able to recognize it as your data?

A. Yes, ma'am.

Q. Can I show you Exhibit 740, which has already been admitted?

Do you recognize what's shown in Exhibit 740?

A. Yes, ma'am. It's the directory listing of an S3 bucket.

Q. Okay. And can you tell us what kind of information is

contained within those buckets?
A. In this specific case, the data that was contained was result -- are survey results that provided phone number, last name, first name, email address, and address of the people we surveyed.
Q. Okay. Approximately, how many customer records or survey records were contained within this data set?
A. 1.2 million.
MS. MANCA: And can we unpublish that and show Exhibit 741?
Q. (By Ms. Manca) Do you recognize what I'm displaying as Exhibit 741?
A. Yes, ma'am. That's the data the FBI provided to us.
MS. MANCA: Your Honor, we offer Exhibit 741.
MR. KLEIN: No objection, Your Honor.
THE COURT: 741 is admitted into evidence.
(Government Exhibit 741 admitted.)
Q. (By Ms. Manca) Okay. So this left-hand column that has a gray bar, is that gray bar something that was in the data set?
A. No, ma'am.
Q. What is the unredacted content of what's on the left?
A. That's a phone number, ma'am.
Q. Okay. And then there are names; whose names are those?
A. Those are the consumers that we would have surveyed.
MS. MANCA: Okay. Can we scroll?

This is page 2.

Page 3.

Okay. Page 4, if we can -- or page 5, can we stop there and highlight that?

Q. (By Ms. Manca) So this particular data set talks about Whirlpool, Maytag, appliances, refrigerators, dishwashers, dryers. Why is that information contained in these records?

A. We did a survey in regards to a maintenance on their appliances and that was the appliance type that they had.

Q. Were you able to calculate the value of this data?

A. Yes, ma'am.

Q. And how did you calculate that value?

A. We took fair market price. The survey data is purchasable and so you can actually go out and buy a list of contacts to do survey management against. We took our best practices and found that it was 20 cents per record if it had an email address, which is the low end of the spectrum.

After interrogating the data, we determined that about 50 percent of them had an email address, so at 600,000 times 20.

Q. And what was the total value then?

A. $120,000.

Q. Okay. How did your company's computer systems typically process this particular data that was stolen?

A. So this data specifically was at rest. It was actually in the S3 bucket as cold storage. It wasn't actually being

realtime processed.

Q. Can you explain what it means to be in cold storage?

A. So cold storage is taken off of the -- taken off of the physical machine that's doing the processing and putting it into a storage device for later use.

Q. So this isn't information that you were typically accessing in the ordinary course of business at this point?

A. Yes, ma'am, that's correct.

Q. Did your company intend for this data to be generally available to the public?

A. No, ma'am.

Q. How do employees access this data in cold storage within your company?

A. So they would have to have an IAM Role that gave them access to the S3 bucket directly, and then they could access it either via the CLI or from the dashboard we spoke about earlier.

Q. And in order to be provisioned with this -- is it AIM or IAM?

A. IAM.

Q. Okay. In order to be provisioned with this IAM Role, who decides who gets which role?

A. Ultimately, it stops at my desk. The request will come in from the management team that's requesting it, at which point we'll make a decision if that employee is deemed to have access to it, if the job requires them to have access to it. And then

we'll provide the credentials, an MFA token to log in.
Q. What are the credentials and the MFA token used for?
A. So it's used to log on either to the web portal or the CLI tool, and it's authentication. And the MFA is just a secondary authentication.
Q. Okay. And so once an employee has the authentication, at that point the employee can assume the IAM Role if you allow them to do so?
A. That's correct, ma'am, yes.
Q. Would an employee use the CICD instance role credential to access this data in the ordinary course?
A. No, ma'am.
Q. Why not?
A. It's used for realtime running only. And the only people to have it are the people that set the machine up to actually do the realtime processing.
Q. Has Paige Thompson ever worked for Survox or Enghouse?
A. No.
Q. Did you intend for her to assume the CICD instance role?
A. No, ma'am.
Q. Did you intend for her to access your company's information?
A. No, ma'am.
MS. MANCA: No further questions. Thank you, sir.
THE COURT: Mr. Klein, any questions for Mr. Roundy?

MR. KLEIN: Yes, Your Honor.

THE COURT: Okay.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good afternoon.

A. How are you, sir?

Q. I represent Paige Thompson.

I'm just going to go over a few things with you that you discussed.

Maybe I'll start here at the end where you were.

You mentioned how the intent is for only employees to have access to some of this data; right?

A. Yes, sir.

Q. But in this case, other people could have access to data the way the system was set up; right?

A. Yes, sir.

Q. You also talked about how your system was set up. I'm turning now to the cryptomining part of this. Do you remember those questions from the prosecutor?

A. She didn't talk directly about cryptomining.

Q. Okay. Do you know that any cryptomining was done on your system?

A. I have no evidence if it was done or not.

Q. Okay. I wanted to talk to you about the data, that's Exhibit 740 and 745. Do you remember those exhibits?

A. No. If you could bring them up again, that would be great.
Q. Sure. We can bring them up for you.
MR. KLEIN: 740, please. We'll try a split screen here. 741.
And that's the royal "we." I will not try to do that because I would not be able to do it.
A. Okay. Yes, sir, I do remember them.
Q. (By Mr. Klein) So you mentioned that you had specific -- at least intention -- you would intend to have only certain employees have access to the data; right?
A. Yes, sir.
Q. But you also talked about how you value this data. And you talked about how you went out and looked at what the fair market value of this data was?
A. Correct, sir.
Q. And you determined that by going to see how much you could purchase data like this for?
A. Yes, sir.
Q. So this type of data is purchasable by people?
A. Not all of the data, but most of it, yes, sir.
Q. So I could -- someone off the street could go to one of these companies that you based your evaluation on and purchase similar type of data?
A. Yes, sir.
MR. KLEIN: Nothing further.

THE COURT: Anything else, Ms. Manca?

MS. MANCA: One question. Thank you.

THE COURT: Sure.

REDIRECT EXAMINATION

BY MS. MANCA:

Q. Why don't you have evidence of whether cryptomining was done on your systems or not?

A. We didn't have any access to the actual platforms to find out what they were doing.

MS. MANCA: No further questions. Thank you.

THE COURT: Thanks, Mr. Roundy. I appreciate it. You're very polite, too. Is that military?

THE WITNESS: No, sir.

THE COURT: Just polite. That's nice.

THE WITNESS: Little nervous.

THE COURT: Oh, no. Your ma'ams and sirs were very much appreciated.

THE WITNESS: You're more than welcome. Thank you.

THE COURT: You've got to say, more than welcome, Your Honor.

THE WITNESS: Yes, sir.

THE COURT: Thank you. You're excused.

THE WITNESS: Thank you.

THE COURT: Okay. This would probably be a good time to take our afternoon break, and we'll come back at 3:00.

So stroll next door and Victoria will come get you a little before 3:00.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: What type of length of witness is Mr. Chamberlin?

MS. CULBERTSON: I would estimate 30 to 45 minutes, Your Honor.

THE COURT: Okay. So that 3:00 to 4:00 should take care of it pretty well.

MS. CULBERTSON: I think so.

THE COURT: Great.

And then tomorrow, Mr. Henderson and Mr. Strand take up the morning, you think?

MS. MANCA: We think probably a little less than the morning, so, yeah.

THE COURT: Okay. So the government will be expecting to rest its case late morning or by noon.

MS. MANCA: I believe that's an accurate estimate, Your Honor.

THE COURT: Okay. And, Victoria, we have a list of exhibits where I've reserved ruling. Do the parties have the updated numbers on those?

THE CLERK: They've all been ruled upon.

THE COURT: They've all been ruled upon. Wonderful.

MS. MANCA: Your Honor, I believe 956 was reserved.

THE CLERK: Except for that one.

THE COURT: 956, which was the chart that I allowed for demonstrative purposes, but you're offering it for substantive purposes.

MS. MANCA: We are, as a summary of records.

MR. KLEIN: Your Honor, we oppose that. The records are not that big. Usually a 1006 summary is massive records. They can use it as a demonstrative, then they can use it in their close, but they don't need it as an actual exhibit.

THE COURT: I'm going to admit 956 into evidence. I believe it's appropriate to have that summary chart in there.

Okay. Now, we still have the Mr. Ho issue.

MR. KLEIN: Your Honor, thank you for sharing the unredacted version. I reviewed it. I don't think we need to recall Mr. Ho at this time, but it does flag the concern I was raising earlier about when Mr. Strand testifies there are -- there was an email portion of that that would have been relevant to my cross-examination, at least to understanding what he was saying, where there was an exchange with the prosecutor and him. And so I would, again, request that we receive unredacted versions of the emails of Mr. Strand.

THE COURT: How many emails are we talking about with Mr. Strand?

MR. KLEIN: I think it's under ten, five or six maybe,

Your Honor. I don't have them in front of me. It's not that many.

THE COURT: Could you take a fresh look at that and see if there's some you could say, yeah, might as well just turn it over.

MS. MANCA: Okay.

THE COURT: Okay. And if not, I'll look at it tomorrow.

MR. KLEIN: Yes, Your Honor.

THE COURT: Okay. So when the government rests its case, you have a motion?

MR. HAMOUDI: Yes.

THE COURT: And who -- you're going to make that, Mr. Hamoudi?

MR. HAMOUDI: Yes, I am, Your Honor.

THE COURT: Okay. And then what about -- if I take it under advisement, are you ready to start tomorrow afternoon?

MR. HAMOUDI: Yeah, Your Honor. We would be ready to start tomorrow afternoon.

THE COURT: Okay. And do you know your likely sequence of witnesses?

(Off the record.)

MR. HAMOUDI: We're still figuring that out.

THE COURT: Okay. All right. When you figure that out, would you please advise the government and Victoria --

MR. HAMOUDI: Absolutely.

THE COURT: -- of your number of witnesses and who's going to do it, and then tell me who's going to do cross.

MR. HAMOUDI: I will do that, Your Honor.

THE COURT: And do you anticipate taking Tuesday afternoon, all day Wednesday, and any further?

MR. HAMOUDI: I suspect, Your Honor, that our case should be complete by Wednesday.

THE COURT: End of Wednesday.

MR. HAMOUDI: I suspect. And I'm just --

THE COURT: Yeah. Yeah. I'm not holding you to it.

MR. HAMOUDI: Okay. Thank you, Your Honor.

THE COURT: I'm just trying to make plans then.

And I want to take enough time to go over the jury instructions fairly carefully, so it helps me to kind of know when you're doing that.

Do you -- who is going to do closing argument?

Mr. Friedman, you've got opening, closing.

MR. FRIEDMAN: I have opening, closing, and then Ms. Manca will do rebuttal.

THE COURT: And then, Mr. Hamoudi, you're going to do closing.

MR. HAMOUDI: I'm going to do closing.

THE COURT: Do you have an expert over there on jury instructions or are you both -- Mr. Klein, you're --

MR. KLEIN: I'm going to handle the charge conference.

THE COURT: Okay. Great.

And, Ms. Manca -- Ms. Culbertson's got that. Okay. Great.

MR. KLEIN: Your Honor, do you know when we might have the charge conference just in terms of timing?

THE COURT: I'm sorry, I didn't hear you.

MR. KLEIN: Do you know when we might have the charge conference, when we might need to discuss --

THE COURT: Oh, the charge conference. Never heard that one before.

The discussion on jury instructions.

MR. KLEIN: Yeah, yeah.

THE COURT: Let's see. Well, Ms. Daugherty is going to give you a revised set. You can email back to her, both sides, on, you know, hey, this isn't right or this.

And then I think we'd probably do maybe Wednesday afternoon 3:00 to 4:00 kind of thing.

And then I'll take those suggestions under advisement. We'll do formal exceptions maybe Thursday morning, and then into closing arguments, and maybe Thursday or Friday, we'll see.

MR. KLEIN: And, Your Honor, we had at least two additional jury instructions we wanted to submit. And for the ones where we, you know, disagree or have a redaction or an edit, should we -- is that something we should submit in advance?

THE COURT: Yes. Because I will look at it. I may make some more adjustments.

MR. KLEIN: Okay. Yeah.

THE COURT: And then in regard to the AWS contracts, if you haven't had a chance to talk to each other, see if you can come up with a stipulation to that model, one that was included in the declaration. And if you can, let's let AWS not worry about anything else on the subpoena, okay?

MR. HAMOUDI: I just need the declaration, Your Honor. I'll grab it.

THE COURT: Yeah, sure. We don't have to decide it right now, but that's where we're heading.

And then in terms of your desire for Capital One witnesses, you got that under control?

MR. HAMOUDI: Yes, Your Honor.

THE COURT: Okay. Wonderful.

So we'll start up again about 3:05, okay?

Great. We'll be adjourned. Thank you.

THE CLERK: Please rise.

(Court in recess 2:49 p.m. to 3:07 p.m.)

THE COURT: Okay. The last witness of the day, Ms. Culbertson?

MS. CULBERTSON: The government calls George Chamberlin.

THE COURT: Mr. Chamberlin, please come forward into

the open area of the courtroom here. Raise your right hand, and my clerk will swear you in.

GEORGE CHAMBERLIN,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and spell your last name for the court reporter.

THE WITNESS: George Chamberlin, C-h-a-m-b-e-r-l-i-n.

THE COURT: Thank you, Mr. Chamberlin.

Go ahead, Ms. Culbertson.

DIRECT EXAMINATION

BY MS. CULBERTSON:

Q. Hi. Good afternoon, Mr. Chamberlin.

A. Hello.

Q. Where do you work?

A. I work at Amazon Web Services.

Q. Do you work at a particular group at Amazon Web Services?

A. I do. I work in a team that assesses fraud risk for AWS services before they're launched, for general availability to the public. The team that I manage, also we do fraud-threat intelligence work to identify emerging fraud trends to protect AWS customers.

Q. And what is your title in that role?

A. I'm a senior risk manager.

Q. How long have you been with AWS?

A. Since August of 2020.

Q. And before that, can you tell me a little bit about your career before you came to AWS?
A. Yeah. I was a Marine officer in the infantry, and then I was in the FBI for just shy of 22 years.
Q. Okay. And just to be clear, were you involved, in any way, in the investigation of this case when you were at the FBI?
A. I was not.
Q. Did you have any contact with any of the FBI case agents on this case about this case while you were at the FBI?
A. No.
Q. When did you first learn about this case?
A. About three weeks ago.
Q. Good enough.

Okay. So let's talk a little bit about risk managers at AWS.

Tell me, again, what does that involve, just generally?
A. So the risk manager -- it is a job family, so a risk manager is brought in to assess and manage risk for many number of different sectors. In my area, it's with fraud, but there can be other risk managers that work in other parts at AWS that mitigate and reduce risk for the company and the customers in other areas of expertise.
Q. So you're using the term "fraud." Can you define that for me?
A. In this context, when I refer to "fraud," I'm referring to

the use of AWS resources without the intent to pay for it. That's the best context.

Q. Can that be by external actors?

A. Yes.

Q. Can that also be internal actors?

A. Yes, it could be.

Q. Do you have a different term that you use when it involves internal actors?

A. We have a different team that manages the internal or insider risk for fraud. Our team is largely focused on the external risks.

Q. So what kinds of things might be worked on by your fraud team?

A. Intentional nonpayment, so the use of compromised credit cards. A fraud actor may use compromised credit cards to open a fraudulent AWS account, launch resources, and then not pay for it, or the person who actually owns the credit card gets the bill. The person may also use a prepaid card that does not have enough money to cover. AWS's is a post-paid model, so we charge after the first month, so there may be more resources that are used and launched than they intended to ever pay for. So that would be another method. It's INP, intentional nonpayment.

We also are involved in account takeovers, legitimate customers who've had their account compromised, so to speak, and have unintended use in their account by the compromised actor,

who may have stolen their credentials or in other ways gotten access to their account.

Q. Let's focus on the term "account takeovers." Why does the fraud team look for account takeovers?

A. We look for that because it impacts our customers. The customers will notify us when they detect unintended use. We also have methods and mechanisms to detect it and will reach out to the customer. So we look for it because of the customer impact that it has.

We also look for it because AWS is a large resource, but it's not an infinite resource, and often the compromised accounts and those that are in them launch a high-scale volume of resources that can impact other customers in those regions.

So we look at it for multiple reasons: Protect the company, protect the customers, and protect the resource.

Q. So when somebody external to an AWS account -- so an external actor -- conducts an account takeover, what things might they be able to do with an account?

A. Can you repeat that last part there?

Q. So if an external actor does an account takeover, what kinds of things might they then be able to do with that account?

A. Okay. So they can have access to the resources that that customer has access to, depending upon their privilege level.

One of those is launch compute resources, and that's what we see very frequently. The compute capacity within AWS EC2 or

Elastic Compute Cloud is one of the resources that can be launched.

Q. Are you familiar with the term "cryptojacking"?

A. Yes.

Q. What does it mean to you?

A. In this context, cryptojacking means stealing resources in order to mine cryptocurrency. You're not paying for the resources that you're using to mine the currency, so you're hijacking that resource in order to conduct cryptomining.

Q. Could somebody just conduct cryptomining on their own account? So, in other words, open an AWS account, and then use the resources in that account that they pay for to do cryptomining?

A. They can, yes. Cryptomining, in and of itself, is not illegal and it's not against AWS's use policies.

Q. Why might somebody cryptojack rather than just cryptomine in their own account?

A. It comes down to profitability. Can you make a profit mining cryptocurrency. So if you don't pay for the resource and you're able to use it for free, then you can make a profit using those resources to cryptomine.

If you're a paying customer and using those resources, you will not make a profit. Depending upon the price of cryptocurrencies, it can fluctuate, but, generally, you won't make a profit if you're paying for the resource.

I do want to clarify one piece.

It's not against AWS's terms of use to cryptomine with the exception of we offer, sometimes, free credits to some customers. When you're given free credits or a free-tier usage, then that is against the policies to use that to cryptomine. Just as a clarification there.

Q. Yeah. Thank you for that.

How does an issue usually come in to the fraud team to be worked on by AWS?

A. The issue would come in either from the customer contacting customer service, and customer service contacting fraud prevention, or we may proactively detect activity indicative of cryptomining as well, and reach out to the customer.

Q. So you mentioned activity indicative of cryptomining. What would be activity indicative of cryptomining in an account?

A. So we look for patterns that -- what I mean by that is, there may be a standard-usage pattern, where a customer launches AWS resources within specific regions or -- so if we detect launches that are outside of that normal pattern of activity using resources that that customer may not normally use, that may be an indication that there's compromised activity. We also look at things like connections and other data around the resource that might be indicative of cryptomining.

Q. Would creation of particular instance types potentially be indicative of cryptomining?

A. It may, along with some other factors, yes.
Q. What about an increase, higher-than-normal usage on an account?
A. Yes.
Q. So when you're talking about certain instance types that could potentially be indicative of cryptomining, what kind of instances does that generally involve?
A. Instances that have higher-capacity compute power, like P family, "P" as is "Paul," P3; G family, "G" as in "golf." We will see those used for cryptomining as well; and sometimes C, C family, as in "Charlie," those are general compute, efficient compute instances sometimes are used in cryptomining as well.
Q. I believe you said "P family." You mentioned "family." So does that mean these instances come in different configurations or different sizes? What does that mean?
A. They do.

So there's many different types of instances, which is virtual computing power in the cloud, so to speak. So you launch an instance. Those instances, depending upon your use case or your workload, you can choose from over 100 different types of instances to be most effective for the job that you want to accomplish.

So AWS calls its instances by families. P is one family, and so it may be, for instance, P316 extra large. That may refer to the third generation of the P family, and then the

size, so 16X large would be a very high-performing, high-capacity instance. It's a large instance.

Another one, like a G, like a G4.4XL may be of the golf or G family. That's for our graphics processing unit. It's for high graphics, gaming, videos, machine learning, high compute, and that it would be -- like, a G4 would be the fourth generation of that G family, and then, once again, the size.

Also within there, there may be another letter, which indicates additional capacity, like memory or storage. So you may see a G4DNXL or something. That would all be indicative of the family, the generation, the capacity, and the size.

Q. So we talked a moment ago about anomalous account activity that might be as to region in an account. How do regions of instances potentially indicate something like cryptomining or cryptojacking?

A. That would be indicative if a customer regularly uses -- when I say "customer," it could be an individual, it could be an enterprise -- regularly uses a region or a group of regions, say a U.S.-based region on the East Coast or one on the West Coast, then there are a series of instance launches in Asia or in eastern Europe, that would be something we'd look at as anomalous, outside the range of the normal patterns of use with the regions.

Q. Does the work that you do on the fraud team require you to review AWS account billing records?

A. Yes.
Q. So is it fair to say that you're quite familiar with AWS account billing records?
A. Yes.
MS. CULBERTSON: Your Honor, at this time, the government has a series of exhibits. I'm going to list them. I've given the court clerk this list, and we're going to seek to admit them in bulk.
THE COURT: Okay.
MS. CULBERTSON: These are all in the 900 series, so I'll read the numbers. They're 905 to 910, 914 to 922, and then 928 and 930.
Some exhibits are spreadsheets with a lot of data, so for ease of reference, we've created versions where relevant fields are highlighted, and those are just for demonstrative purposes.
So those would be 923 through 927, 929 and 931. And we would ask to admit those only as demonstratives.
Q. (By Ms. Culbertson) Mr. Chamberlin, have you, prior to your testimony today, reviewed the exhibits I just listed?
A. Yes.
Q. Can you give us a general overview of what these exhibits are?
A. So these would be invoices that are sent to the customer on usually a monthly basis. It's called an anniversary billing cycle. So it would be invoices.

And then they would also be potentially credit memos or credit invoices, depending upon the time within the month that a potential unintended use was brought to our attention or the customer detected it.

So these are basically communications that go out to the customer from the AWS Billing.

Q. And do the exhibits I listed also include some spreadsheets?

A. Yes.

Q. And what are those, generally speaking?

A. So the spreadsheets are extracts of data that's kept by AWS within our billing console.

Q. Okay. So were these exhibits or the data -- the excerpts of the data shown in the exhibits made by a person with knowledge of or made from information transmitted by a person with knowledge of the acts and events appearing in them?

A. Yes, they were.

Q. Were the records made at or near the time of the acts and events appearing on them?

A. Yes.

Q. Is it Amazon's practice to make such records?

A. Yes.

Q. Were they kept in the source of a regularly conducted business activity?

A. Yes.

MS. CULBERTSON: Your Honor, the government is moving to admit these exhibits.

THE COURT: So 905 to 910, any objection, Mr. Klein?

MR. KLEIN: Not to those, Your Honor.

THE COURT: Okay. 905 through 910 admitted into evidence.

(Government Exhibits 905 to 910 admitted.)

THE COURT: All right. 914 to 922?

MR. KLEIN: No, Your Honor.

THE COURT: All right.

(Government Exhibits 914 through 922 admitted.)

THE COURT: And the last two are 928 and 930.

MR. KLEIN: Your Honor, I don't have these in my binder. I'll look, but, provisionally, I think they're fine. I don't think I have a problem with them, though.

THE COURT: Are you also moving the demonstrative exhibits?

MS. CULBERTSON: I am.

THE COURT: Those are demonstrative only.

MR. KLEIN: Oh, okay. Then I have less of a problem.

THE COURT: Not 928 and 930, but the later ones, which I didn't write down.

(Government Exhibits 929 and 930 admitted.)

MS. CULBERTSON: Yeah, it's 924 through 927, and then 929, 931, and 932.

THE COURT: Okay. 924 through 927 are admitted for illustrative purposes and can be displayed.

(Government Exhibits 924 through 927 admitted.)

THE COURT: And then 929 and 931 --

MS. CULBERTSON: And also 932.

THE COURT: -- and 932 are also admitted for illustrative purposes, and if you have any problems, let me know.

MR. KLEIN: Okay.

MS. CULBERTSON: Thank you.

(Government Exhibits 929, 930, 932 admitted.)

THE CLERK: May I clarify? Did you list 923 initially as one of the demonstratives?

MS. CULBERTSON: Oh, I'm sorry. That should be "923," not "932." I switched the digits. Thank you for catching that.

THE COURT: Good catch, Victoria.

So 923 instead of 932.

(Government Exhibit 923 admitted.)

Q. (By Ms. Culbertson) Showing you Exhibit 956, it has been admitted, have you seen this document before?

A. Yes.

Q. Do you see on here a customer name "Survox," and it says "Enghouse" in parentheses?

A. Yes.

Q. And then an Amazon account number?

A. Yes.
Q. Okay. So these account numbers are long. I think I'm just going to refer to them by the last four digits. So that's 0924; is that correct?
A. Yes.
Q. I'm going to turn now to Exhibit 923.
Do you see that number ending in 0924 on this spreadsheet?
A. Yes.
Q. So what is this spreadsheet, generally speaking?
A. This spreadsheet is an extract of billing data that we referred to earlier, from our billing console, for this particular account ending in 0924.
Q. I'm going to have you orient us to the spreadsheet a little bit, and explain to us what some of these fields are.
What does column D of the spreadsheet show?
A. That is the AWS service that is being billed.
Q. So that's Amazon EC2?
A. Yes, Amazon EC2 for that row.
Q. What does column E denote?
A. Column E denotes the usage, the billed usage, and whether there was a refund or a credit based upon a business decision by AWS and communication with the customer.
Q. What is the difference between a credit and a refund?
A. So a credit is more forward looking, depending on when in the billing cycle this is detected.

A refund is generally indicative of a customer who has already paid for the service, but they paid for unintended use, and so AWS is doing a billing adjustment and giving them a refund for what they've already paid.

Q. And you mentioned some of these records we're going to be looking at are going to be invoices.

So are credits and refunds reflected differently in those invoices?

A. Yeah. Well, it would be a credit or, potentially, a refund, or a waive. Some fees are waived as well, yes.

Q. Looking at column F, what does that show?

A. So that's the start of the billing cycle in question. You notice each one starts at the first of the month. So that would be March 1st, 2019, or April 1st, 2019.

Q. And column H, what does that show?

A. That's the region that the resource was launched in, as we were discussing earlier.

Q. Okay.

Finally, on the screen, column J. What does that show?

A. So once again, that will show the region, and then it will show the type of instance that was launched, the resource.

Q. Okay. And so that -- here, you see some P38X large, some of those kinds of instances we were just talking about?

A. That's correct, yeah.

And "box usage" is just a metering event that starts at the

top of the instance billing hour, yes.
Q. Okay. Let's go look at column K. What does column K show?
A. That's the instance usage and, usually, in instance hours.
Q. And column L?
A. Those would be the charges.
Q. So we see some charges that are highlighted in yellow, and then others that have a minus symbol in front of them. What do those show?
A. Those would show either credits or refunds back to the customer.
Q. Okay. So because we saw the account number ending in 0924 -- that's Survox's account number -- does this spreadsheet reflect billing information for that customer?
A. Yes.
Q. Having reviewed this spreadsheet, are there indicators that might cause you to suspect anomalous account behavior, as we discussed earlier?
A. Yes. The "P3." If the customer would not normally use P3, they are a high-capacity instance, that would be an indicator. And then, potentially, the region, if the region wasn't normally used by the customer, that would be another indicator.
Q. Do you know, did AWS consult with Survox about this usage?
A. Yes.
Q. Why were billing adjustments ultimately made for Survox in these months?

A. AWS verified, through communication with the customer and also through the indicators that I've just discussed, and reached a business decision to reimburse the customer for the unintended use.

So this would be -- there was a process for communicating with the customer, verifying that the account has been sanitized, meaning that it's not still compromised, and then we will -- a billing adjustment was made based upon that decision.

Q. Do you know, based on this spreadsheet, about how much was made in billing adjustments, either refunded or credited to Survox?

Q. I'm sorry. Can you ask that question again?

A. Based on this spreadsheet, do you know about how much was refunded or credited to Survox?

A. Total, with Survox, from about -- close to $60,000 were the billing adjustments.

Q. So when Amazon refunds, for instance, usage, does it have out-of-pocket costs for providing that resource that then is not covered?

A. Yes, we do.

Q. And that's just out-of-pocket costs. So we're not talking about lost profit; we're just talking about costs to Amazon?

A. That's correct. That's just how much it costs Amazon to run the resource.

Q. In the case of Survox in March and April of 2019, about how

much was that loss to Amazon due to the refunds?
A. So the loss is what we refer to as "operational expenditure," what it actually costs us to run the service, and it was approximately $14,600.
Q. And you said "operational expenditures"; is that right?
A. Yes.
Q. Or expenses.
What pieces make up that expenditure?
A. So it's a marginal cost based upon the infrastructure: So everything from the electricity, the hardware, the degradation of the hardware, the wear and tear, the replacement costs, that all gets factored in to how much it costs to deliver the service.
Q. We're going to turn back to Exhibit 956, quickly.
Do you see a customer named A T Works on here with an account number ending in 4197?
A. Yes.
MS. CULBERTSON: Let's pull up Exhibit 918, please, and if we could, for now, blow up the first half of the page.
Q. (By Ms. Culbertson) And so here we see the account number ending in 4197 and the name A T Works.
What is this document that we're looking at?
A. So this is an invoice to this customer for charges from March 1st through the 31st of 2019.
Q. Okay. And let's back out of it a little bit, and then

let's go to page 2.

Do you see a section on here that says "Amazon Elastic Compute Cloud"?

A. Yes.

Q. And what is the charge there?

A. $20,316.35.

Q. Okay. Let's pull up Exhibit 919. What is this document?

A. So this is a credit memo for that same billing period, March 1st to March 31st, which was sent to the customer in April of 2019, on April 24th, the date.

Q. Okay. And under "detail," we see Amazon Elastic Compute Cloud, and that number in the parentheses, what is that?

A. That's the credit that was given -- the billing adjustment back to the customer.

Q. Okay. So that's $18,375.05?

A. Yes.

Q. Turning now to Exhibit 920, what is this document?

A. This is an invoice for the April 1st to April 30th, 2019, billing period.

Q. Okay. And for the same customer, A T Works?

A. Yes.

Q. And on page 2, again, under Amazon Elastic Compute Cloud, so EC2, what is the charge for EC2 here?

A. Charges are $6,950.61. That's the --

Q. Okay. Sorry. I didn't mean to cut you off.

And we also see, in brackets, $5,208.27. What is that?
A. That's the credit back to the customer for billing adjustment.
Q. So, here, what does it mean that we're seeing both the charge and the credit back in the same document?
A. It means that the customer -- it's a credit memo, so it means the customer was given back, basically, that amount that they were originally charged, so reducing the overall charge to $1,881.73.
Q. As to invoices and credit memos we just looked at for these two months, how much did Amazon refund, approximately, to A T Works?
A. For A T Works, in this invoice it would be $5,208.
Q. Okay. So that's for April.
Do you remember the number for March? We can pull that exhibit back up.
A. Yes. Approximately $23,000.
Q. For two months?
A. Uh-huh.
Q. Turning to Exhibit 924, again, do you see that Amazon account number ending in 4197?
A. Yes.
Q. So does this spreadsheet show billing information for the A T Works account?
A. Yes, it does.

Q. Start date for billing cycle is in column F, and then let's look at column H. Again, tell me what column H shows.
A. Column H is the region that the resources were launched in.
Q. What is different about the ones that are highlighted that goes through row 19 versus the ones that are visible underneath?
A. The region codes are different, showing "IAD," which is in the United States, in Virginia, and "PDX," which is on the West Coast in Oregon, and then row 20, it starts with "NRT," which is in Tokyo.
Q. And then looking at column J, we see, again, a lot of P3 instances here?
A. Yes.
Q. Okay. And then turning to column L. And, again, remind me what column L would show.
A. So those are the charges for the resource usage, based upon the usage total.
Q. Having read this spreadsheet, do you see indicators here that might cause you to suspect anomalous account behavior?
A. Yes.
Q. And what are those?
A. The region, as we just highlighted, and then also the instance family of P3s.
Q. So fair to say billing adjustments, $23,000 worth, were made for A T Works in these two months. Why were these billing adjustments made?

A. It was a business decision. Once again, with assessing the usage and communication with the customer, and after a decision by the billing team and the finance, a billing adjustment was made because it was -- yeah, it was within Amazon business policies.

Q. Okay.

So, again, presumably, Amazon has out-of-pocket costs for these reasons?

A. Yes.

Q. Do you know, for A T Works, approximately what the out-of-pocket cost that was lost to Amazon was?

A. Once again, the op ex, operational expenditure, was approximately $6,700.

Q. Okay. Thank you. We'll go through just a few more of these with a few more customers. I'll try to move through them quickly, because I think we're all kind of seeing how these documents work.

Can we pull up, again, quickly, Exhibit 956?

Do you see PowerSquare India with an account number ending in 7507?

A. Yes.

Q. Let's pull up Exhibit 915. Is this a PowerSquare invoice for March 1st through 31st, 2019?

A. Yes.

Q. Turning to page 2, under "Elastic Compute Cloud," is that a

charge for $17,553.13?
A. Yes.
Q. Turning now to Exhibit 916, is this a credit memo for that same customer, PowerSquare India, for that same billing cycle?
A. Yes, it is.
Q. Okay. And how much is the credit shown here?
A. $17,499.38.
Q. And, again, that's under "EC2"?
A. That is, yes.
Q. Let's quickly pull up Exhibit 917.
And this is the invoice or account summary for billing period April 1st through April 30th, 2019, again for PowerSquare; is that correct?
A. Yes.
Q. Okay. And then on page 2, under "Elastic Compute Cloud," what are we seeing here for charges and credits?
A. So the charges are $1,712.63, and there were credits for $1,668.48.
Q. So as to these two months, March and April of 2019, how much, approximately, did Amazon refund to PowerSquare India for its EC2 usage?
A. Approximately $18,000, $19,000.
Q. Thank you for doing all this math. I appreciate it.
And turning quickly to Exhibit 926, scrolling to the left, do you see the account number ending in 7507?

A. Yes.
Q. The column showing start date of billing cycle, March 1st to April 1st, 2019?
A. Yes.
Q. Region code in column I?
A. Yes.
Q. And then column J, the usage unit?
A. Yes.
Q. Again, what kind of instances are we seeing here?
A. Those are P3-family instances.
Q. And those are high-compute instances?
A. They are. They're high-compute, high-capacity instances with GPUs.
Q. And then column L, I assume, shows charges, refunds, and credits?
A. Yes.
Q. Having reviewed this spreadsheet, are there indicators that might cause you to suspect anomalous account behavior on this account?
A. Yes, there are. The use of the P3s, if it's out of the customer's usual pattern, which it was, and the region as well.
Q. So, you said, Amazon refunded approximately $19,000?
A. Yes.
Q. What were Amazon's out-of-pocket costs that weren't covered as a result?

A. Approximately $4,400, the op ex costs.
Q. Okay. Quickly, back to Exhibit 956. Do you see a customer name here, Waitrainer, in the middle of the page with an account number that ends in 3625?
A. Yes.
Q. Let's call up Exhibit 914, please.
So here we see an account number that ends in 8421. And I'm going to clarify that with you when I call up the spreadsheet, but just quickly looking on page 2 of this exhibit, how much do we see for Amazon EC2?
A. The charges were $8,800 -- $8,894.41.
Q. And how much in credits?
A. The credits were $1,581.55.
Q. And that is for the billing cycle of April of 2019?
A. Yes.
Q. Okay. And we'll call up Exhibit 929, please.
Scrolling all the way over to the left, here we see -- column B says, "payer account ID," and that ends in 8421; is that correct?
A. Yes.
Q. Is that the number that we saw on the invoice that we were just looking at?
A. Yes.
Q. Okay. And under "linked account ID," we see the number ending in 3625?

A. That's correct.
Q. Is that correct?
A. Yes.
Q. And that is the account number we saw on the one-pager that was listing all different account names; is that correct?
A. Yes.
Q. So are these two accounts, essentially, connected under the same account user, Waitrainer?
A. Yes. They're connected pretty much as the name applies. There is a payer account, which actually pays the bills, and then a linked account underneath that payer account. So in this particular case, the billing adjustment went back to the payer account.
Q. Okay. Thank you for explaining that.
So looking on this spreadsheet, column F, that is, I assume, the start of the billing period, as it says up there?
A. Yes.
Q. Column G, here we're seeing the end date of the billing cycle, which we haven't always seen on these spreadsheets. And then scrolling over to column P, here again we're seeing instance type?
A. Yes.
Q. What is an M5 large?
A. It's just another instance type that's listed. It's usually either -- I can't recall exactly what the specifications

of that particular instance are for, but it's generally a general-compute-type instance.

Q. And here we're also seeing another column that we haven't necessarily seen on the other spreadsheets. It says "run instances." What do you understand that to mean?

A. As it states, the instances have launched or they're running, they're live.

Q. Okay. And then in column S, row 5, it says, "unauthorized usage, compromised account." What does that mean to you?

A. This is a notation for -- from a customer communication, and a verification through AWS review, that this was an unauthorized usage of the customer's resources. It's also referred to as "unintended use." In this case, the note refers to unauthorized use.

And the ticket and case ID refers to a support case that was opened to engage with the customer and resolve the issue, and that ID number is the ticket that references the communication with the customer and the actions taken.

Q. Okay. Great.

And then scrolling all the way over to column Z, in row 5. So, again, is that showing the $1,581.54 that was refunded back to the customer?

A. Yes.

Q. And, presumably, in that number, there is some out-of-pocket costs to Amazon?

A. Yes.
Q. All right. We're going to look at one more. Let's pull up Exhibit 956 one last time.
Do you see Hewlett-Packard, Incorporated with the account number ending in 9728?
A. Yes.
Q. Okay. Let's turn to Exhibit 921, please.
Is this an invoice for Hewlett-Packard -- I'll just call them "HP," -- HP, Inc. for April 1st to April 30th, 2019?
A. Yes.
Q. And that's a big invoice. Safe to say they're a big customer?
A. They are.
Q. And pulling up the document -- I'm sorry, on page 9 of that document, in the middle of the page there, we see a charge for EC2. How much is that charge?
A. That charge is $286,816.80.
Q. Okay. And, finally, turning to Exhibit 922, please. This is an HP credit memo for that same month, April 1st to 30th, 2019?
A. Yes.
Q. And how much is credited back for Amazon Elastic Compute Cloud?
A. $9,244.00.
Q. Fair to say, again, that Amazon would not have recouped

some of the costs for the use of the instance it refunded?
A. Right. We have operational expenditure, yes.
Q. All right.
So we have just reviewed a lot of credits and refunds that Amazon made because it determined there were unauthorized instances being run in compromised accounts; is that correct?
A. Yes.
Q. In addition to issuing refunds, what else does Amazon do when it identifies unauthorized instances in communication with its customers?
A. We work with the customer to sanitize the account, protect the account, and we terminate the unintended resources that were not legitimately being launched by the paying customer.
Q. When you say "terminated," does that mean shutting down the instance?
A. Yes.
Q. Can AWS themselves also shut down unauthorized instances that are being run in their accounts?
A. They can.
Q. What records remain for an instance after it has been terminated? And when I say "remain," I say remain with AWS.
A. Largely, the metadata around the instance. It would be what you've just seen here in these exhibits, when it was launched, how long did it run for, what region, the type. This is what we refer to as metadata around that instance, the

instance ID, that will remain.

Q. So, essentially, a fair amount of the information we just looked at in these spreadsheets?

Is anything else left for the instance, in practical terms?

A. No.

Q. So in all of these customer cases we've looked at, based on what you know about those cases and the information we've just looked at together, are you able to draw any inferences about what these instances were -- these unauthorized instances were being used for?

A. Cryptomining. I mean, the type of instance, the fact that the instances were launched in parallel, and the type of instances used are indicative of cryptomining.

Q. And because these instances were shut down by AWS or by the customer, working together, is it fair to say that that cryptomining was unauthorized?

A. Yes.

Q. So it could be called "cryptojacking"?

A. Yes.

MS. CULBERTSON: Okay. Nothing further. Thank you.

THE COURT: Thanks, Ms. Culbertson.

Mr. Klein will have some questions for you now.

MR. KLEIN: Your Honor, I'm going to go longer than 4:00.

THE COURT: Go ahead and get started. We might go a

little past 4:00 today, if that's okay with everybody.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good afternoon.

A. Good afternoon.

Q. I'm going to walk you back through some of your testimony. I have some questions about it.

I'm Brian Klein. I represent Ms. Thompson.

So you ended up your testimony talking about refunds and your conclusions.

Did you ever speak, personally, to any of these customers?

A. I did not.

Q. Did you rely on what others at Amazon told you?

A. For the data, yes.

Q. Did you ever -- when you looked at the data, the data that you're looking at here, the time period is only from February to September, isn't it?

A. Yes. Yes.

Q. Okay. So you didn't look in January of 2019 or in October of 2019?

A. No.

Q. Didn't look at 2018 at all?

A. No.

Q. Didn't look at 2020?

A. No.

Q. And the customers you talked about -- and I direct your attention to Exhibit 926.

MR. KLEIN: If we can pull that up, please.

Is that 926? 956. Apologies.

Q. (By Mr. Klein) Customers, when they sign up for AWS, can sign up for more than one AWS account, yes?

A. Yes.

Q. So, for example, Hewlett-Packard might have multiple accounts.

A. They may. I don't know if they do or not, but they may.

Q. You were only asked to look at one of their accounts, correct?

A. Yes.

Q. So they might have other accounts, right? And the account you looked at, actually, was just one for Hewlett-Packard in Puerto Rico. I direct your attention to Exhibit 921. Is that a Puerto Rico-based account, at least based on the address at the top left-hand corner?

A. Yeah -- well, the billing is, right? So fair enough, yeah.

Q. You only looked at this very specific one?

A. That's correct.

Q. And customers can move resources around between accounts, can't they? So they can have, let's say, two accounts, and move a resource from one account to another account, correct?

A. Generally, yes, depending upon region restraints, but, yes,

generally.

Q. So they can decide, Hey, we're going to run something on this account, but now we're going to run our -- and I'm going to use the word I think you used -- the P instance, so they could launch a P instance on one account, and then decide to open it up and use it on another account, right?

A. Well, the account would be billed under the account which it was opened under, right?

Q. So you only looked at one account for this company, right?

A. Yes.

Q. Okay. And you only looked for a time period from February to September 2019?

A. Yes.

Q. And that's the same for all the accounts you looked at? You just looked at one single account for that company.

Let me move forward.

The refunds you talked about, were you personally involved in those refunds?

A. No.

Q. So this is just what you learned from others?

A. Well, I want to just say -- I'm not being -- contesting -- but when I say "learned from others," it's looking at the records and the data. That's what I've learned from, not necessarily talking to others. Just to clarify.

Q. That's helpful. I appreciate it.

So when you looked at the records, you could see a refund was given?

A. Yes.

Q. You weren't involved in the decision to make the refund, though, were you?

A. No.

Q. The first time you spoke with anybody about this case was just -- you just said -- was three weeks ago?

A. Uh-huh, yes.

Q. And you've looked at the records shown to you by the prosecutor, but you haven't done your own independent review of records, have you?

A. No.

Q. AWS customers get refunds for a lot of reasons, don't they?

A. There's a business-decision process. I wouldn't say there is a lot of reasons. There are reasons for refunds, but there is a decision-making process that goes into each one. So, yes.

Q. And that's an Amazon internal determination?

A. It is, yes. It is a business decision, yes.

Q. When you say "business decision," is that sometimes done to maintain the customer relationship?

A. It's done for that reason. It may be done also to -- it may be for the customer relationship, yes.

Q. And customers ask for refunds for many different reasons, or, at least, some, typically?

A. Customers ask for refunds for different reasons, yes.
Q. And you don't actually know if any cryptomining was done on any of these specific accounts, do you?
A. No, I didn't investigate. I wasn't part of this investigation.
Q. Okay.
And you mentioned earlier that AWS -- I'm going to use "Amazon" sometimes, I apologize, but I'll use AWS to be specific -- has resources that its customers can deploy, right?
A. Yes.
Q. And AWS is huge. What is its revenue, approximately?
A. It is a lot.
Q. Billions?
A. It's in the billions, yes.
Q. And in terms of the number of servers it deploys for customers, what is the estimate?
A. I wouldn't even give an estimate in terms of the number of servers.
Q. Tens of thousands?
A. There's thousands, yes. There's regions all over the world.
Q. So the deployment of resources here, the refunds here you're talking about, didn't affect the available resources for these customers or anybody else at AWS; these are very small amounts, right?

THE COURT: I'm not sure what that question means. Maybe you can rephrase it.

MR. KLEIN: Yes, Your Honor. I'm trying to get to the idea --

THE COURT: I didn't say I didn't understand where you're trying to get to.

THE WITNESS: Your Honor, I think I --

THE COURT: Okay.

A. So in terms of revenue, these are small amounts, but there is another reason that these are also investigated, and that's capacity. So these can have impact on capacity for other customers in those regions.

Q. (By Mr. Klein) But you don't know that because you weren't involved in the investigation, were you?

A. No, I was not involved in the investigation.

Q. If you had gotten involved in this investigation in 2019, there would have been CloudTrail logs available at that time, right?

A. Yes.

Q. You haven't seen any CloudTrail logs, have you?

A. No.

MR. KLEIN: One second, Your Honor. I think I'm done. Nothing further.

THE COURT: Okay. Ms. Culbertson?

MS. CULBERTSON: Nothing further.

THE COURT: We almost nailed it at exactly four o'clock.

Ladies and gentlemen, we are moving slightly ahead of schedule, I would say. We're going to have -- and sometimes when we get to certain points of the trial, like when the government rests its case, which might take place as early as tomorrow by lunchtime, I sometimes have to take some matters up outside the presence of the jury. So we need to be a little flexible on both sides in the next couple of days.

I may be sending you home earlier. I may be extending your lunch. I just can't tell right now. But the thing I really can say to you, is we will have this case to you submitted to the jury, I would, say by Thursday for your decision. So in that sense, I think we're running well ahead of schedule.

I do want you to keep an open mind. Don't form any conclusions until you've not only heard all the evidence but you get the court's instructions to the jury and the closing arguments of counsel.

And, again, don't do any research, don't do any checking up on anyone involved in the case.

Tomorrow, if you'll come in, I would say 8:50, we'll try to get started promptly at nine o'clock. And once the government has rested its case, I'll know a little bit better about where we're headed for the rest of the day. But flexibility is our code word for the next couple of days.

Great. So you are excused. Leave your notepads and pens on your chairs, and we'll see you tomorrow morning.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Thank you. Please be seated.

Okay. Miss Daugherty is going to send out another slightly adjusted version of the jury instructions. I had her look at some of my previous ones about sequencing and combining a few.

If you have matters you want to go back to her, you have her email addresses, I think, on both tables. You can send her, hey, what about this or what about that, but it will all come to me, eventually.

In regard to that sample contract, have you had a chance to look at that, and is that going to be okay, Mr. Hamoudi?

MR. HAMOUDI: I spoke with Mr. Newby, and I asked them to come up with some language about what I need to establish, because they're familiar with their contracts, I'm not, and then I was going to forward that language to the government and hopefully, get a stipulation.

THE COURT: Good. That's great. Okay.

And then, Ms. Manca, you're going to look at some of those redactions.

MS. MANCA: Yes, Your Honor.

THE COURT: And let them know if there is more paper you can send their way.

Anything else?

MR. HAMOUDI: Your Honor, if I may ask Miss Daugherty if we can have a Word version of the instructions, it would be easier for us to respond. Just to make clear, if we want to add or modify instructions, we can send it directly to her and cc the government?

THE COURT: Yes, that would be great.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Mr. Klein?

MR. KLEIN: Your Honor, the motion to quash for Mr. Nehr, N-e-h-r, I believe, we're not going to call that person, so I don't think --

THE COURT: Okay. We're talking about the witness tomorrow.

Anything from the government, Mr. Friedman?

MR. FRIEDMAN: No, Your Honor.

THE COURT: Very productive day. We'll be adjourned. We'll see you tomorrow morning. We will start at 9:00.

(Proceedings adjourned at 4:05 p.m.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 13th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter